

[Name of Document] Application for Patent

[Reference No.] 0290580314

[Date of Filing] November 20, 2002

[Addressee] Commissioner of the Patent Office

[Int. Cl.] H04L 9/14

[Inventor]

[Address] c/o Sony Corporation, 7-35, Kitashinagawa
6-chome, Shinagawa-ku, Tokyo

[Name] Susumu SENSU

[Applicant for Patent]

[Id. No.] 000002185

[Name] Sony Corporation

[Agent]

[Id. No.] 100082131

[Patent Attorney]

[Name] Yoshio INAMOTO

[Phone No.] 03-3369-6479

[Application Fees]

[Prepayment Registration No.] 032089

[Amount of Payment] 21000

[List of Documents Attached]

[Name of Document] Specification 1

[Name of Document] Drawings 1

[Name of Document] Abstract 1

[No. of General Power of Attorney] 9708842

[Proof]

Required

[Name of Document] SPECIFICATION

[Title of the Invention] RECORDING SYSTEM AND METHOD,
RECORDING APPARATUS AND METHOD, INPUT DEVICE AND METHOD,
PLAYBACK APPARATUS AND METHOD, RECORDING MEDIUM, AND
PROGRAM

[Claims]

[Claim 1] A recording system in which an input device and a recording apparatus are connected to each other via a bus, said input device comprising determination means for determining whether input content is to be protected,

said recording apparatus comprising recording means for recording on a recording medium, together with the content, protection information indicating whether the content is to be protected when being transmitted on the bus based on a determination result obtained by said determination means.

[Claim 2] A recording system according to claim 1, wherein said recording means records the protection information in predetermined units of the content.

[Claim 3] A recording system according to claim 2, wherein the predetermined unit is 2048 bytes.

[Claim 4] A recording system according to claim 1, wherein said recording apparatus further comprises encryption means for encrypting the content by using an ID and a recording medium key of the recording medium when said determination means determines that the content is to be

protected.

[Claim 5] A recording system according to claim 1, wherein said recording apparatus further comprises encryption means for encrypting the content by using at least a recording medium key of the recording medium when said determination means determines that the content is not to be protected.

[Claim 6] A recording system according to claim 1, wherein each of said input device and said recording apparatus further comprises authentication means for authenticating each other.

[Claim 7] A recording system according to claim 1, wherein:

said input device further comprises first encryption means for encrypting the content before being sent to the bus when said determination means determines that the content is to be protected; and

said recording apparatus further comprises second encryption means for encrypting the content before being recorded by said recording means when said determination means determines that the content is to be protected.

[Claim 8] A recording system according to claim 7, wherein said first encryption means prohibits the content from being encrypted before being sent to the bus when said determination means determines that the content is not to be

protected.

[Claim 9] A recording method for a recording system in which an input device and a recording apparatus are connected to each other via a bus, wherein:

said input device determines whether input content is to be protected; and

said recording apparatus records on a recording medium, together with the content, protection information indicating whether the content is to be protected when being transmitted on the bus based on a determination result.

[Claim 10] A recording apparatus for recording information on a recording medium, comprising:

authentication means for conducting mutual authentication with another apparatus connected to said recording apparatus via a bus;

decryption means for decrypting content encrypted with a first encryption method and supplied from the another apparatus via the bus; and

recording means for recording on the recording medium, together with the content decrypted by said decryption means, protection information indicating that the content is to be protected when being transmitted on the bus.

[Claim 11] A recording apparatus according to claim 10, further comprising encryption means for encrypting the decrypted content with a second encryption method.

[Claim 12] A recording apparatus according to claim 11, wherein said encryption means encrypts the decrypted content by using an ID and a recording medium key of the recording medium.

[Claim 13] A recording apparatus according to claim 10, wherein said recording means records the content together with protection information indicating that the content is not to be protected when being transmitted on the bus when the content supplied from the another apparatus via the bus is not encrypted with the first encryption method.

[Claim 14] A recording method for a recording apparatus which records information on a recording medium, comprising:

- an authentication step of conducting mutual authentication with another apparatus connected to said recording apparatus via a bus;

- a decryption step of decrypting encrypted content supplied from the another apparatus via the bus; and

- a recording step of recording on the recording medium, together with the content decrypted by processing of said decryption step, protection information indicating that the content is to be protected when being transmitted on the bus.

[Claim 15] A recording medium for recording therein a computer-readable program for a recording apparatus which records information on a recording medium, said computer-readable program comprising:

an authentication step of conducting mutual authentication with another apparatus connected to said recording apparatus via a bus;

a decryption step of decrypting encrypted content supplied from the another apparatus via the bus; and

a recording step of recording on the recording medium, together with the content decrypted by processing of said decryption step, protection information indicating that the content is to be protected when being transmitted on the bus.

[Claim 16] A program for a recording apparatus which records information on a recording medium, comprising:

an authentication step of conducting mutual authentication with another apparatus connected to said recording apparatus via a bus;

a decryption step of decrypting encrypted content supplied from the another apparatus via the bus; and

a recording step of recording on the recording medium, together with the content decrypted by processing of said decryption step, protection information indicating that the content is to be protected when being transmitted on the bus.

[Claim 17] An input device into which content is input, comprising:

authentication means for conducting mutual authentication with a recording apparatus connected to said input device via a bus;

first encryption means for encrypting the content with a first encryption method according to whether the input content is to be protected when being transmitted on the bus; and

supply means for supplying the content encrypted by said first encryption means to said recording apparatus via the bus.

[Claim 18] An input device according to claim 17, further comprising second encryption means for encrypting the content encrypted by said first encryption means with a second encryption method.

[Claim 19] An input device according to claim 18, wherein one of said first encryption means and said second encryption means encrypts the content by using an ID and a recording medium key of a recording medium.

[Claim 20] An input method for an input device into which content is input, comprising:

an authentication step of conducting mutual authentication with a recording apparatus connected to said input device via a bus;

an encryption step of encrypting the content according to whether the input content is to be protected when being transmitted on the bus; and

a supply step of supplying the content encrypted by processing of said encryption step to said recording

apparatus via the bus.

[Claim 21] A recording medium for recording therein a computer-readable program for an input device into which content is to be input, said computer-readable program comprising:

- an authentication step of conducting mutual authentication with a recording apparatus connected to said input device via a bus;

- an encryption step of encrypting the content according to whether the input content is to be protected when being transmitted on the bus; and

- a supply step of supplying the content encrypted by processing of said encryption step to said recording apparatus via the bus.

[Claim 22] A program for an input device into which content is input, comprising:

- an authentication step of conducting mutual authentication with a recording apparatus connected to said input device via a bus;

- an encryption step of encrypting the content according to whether the input content is to be protected when being transmitted on the bus; and

- a supply step of supplying the content encrypted by processing of said encryption step to said recording apparatus via the bus.

[Claim 23] A playback apparatus for playing back content from a recording medium and for supplying the content to another apparatus via a bus, comprising:

 playback means for playing back from the recording medium the content and protection information indicating whether the content is to be protected when being transmitted on the bus; and

 output control means for controlling the output of the content to the another apparatus via the bus based on the protection information played back by said playback means.

[Claim 24] A playback apparatus according to claim 23, wherein the protection information is recorded in predetermined units of the content.

[Claim 25] A playback apparatus according to claim 24, wherein the predetermined unit is 2048 bytes.

[Claim 26] A playback apparatus according to claim 23, further comprising:

 authentication means for authenticating the another apparatus; and

 encryption means for encrypting the content,

 wherein said encryption means encrypts the content before being sent to the bus when the protection information indicates that the content is to be protected when being transmitted on the bus and when the another apparatus is authenticated by said authentication means.

[Claim 27] A playback apparatus according to claim 26, wherein said output control means prohibits the content from being output to the bus when the protection information indicates that the content is to be protected when being transmitted on the bus and when the another apparatus is not authenticated by said authentication means.

[Claim 28] A playback method for a playback apparatus which plays back content from a recording medium and supplies the content to another apparatus via a bus, comprising:

a playback step of playing back from the recording medium the content and protection information indicating whether the content is to be protected when being transmitted on the bus; and

an output control step of controlling the output of the content to the another apparatus via the bus based on the protection information played back by processing of said playback step.

[Claim 29] A recording medium for recording a computer-readable program therein for a playback apparatus which plays back content from the recording medium and supplies the content to another apparatus via a bus, said computer-readable program comprising:

a playback step of playing back from the recording medium the content and protection information indicating

whether the content is to be protected when being transmitted on the bus; and

an output control step of controlling the output of the content to the another apparatus via the bus based on the protection information played back by processing of said playback step.

[Claim 30] A program for a playback apparatus which plays back content from a recording medium and supplies the content to another apparatus via a bus, comprising:

a playback step of playing back from the recording medium the content and protection information indicating whether the content is to be protected when being transmitted on the bus; and

an output control step of controlling the output of the content to the another apparatus via the bus based on the protection information played back by processing of said playback step.

[Detailed Description of the Invention]

[0001]

[Technical Field of the Invention]

The present invention relates to recording systems and methods, recording apparatuses and methods, input devices and methods, playback apparatuses and methods, recording media, and programs. More particularly, the invention relates to a recording system and method, a recording

apparatus and method, an input device and method, a playback apparatus and method, a recording medium, and a program in which content can be flexibly protected based on whether or not the content should be protected.

[0002]

[Description of the Related Art]

In a recording/playback apparatus (for example, a CD-RW drive), when recording or playing back content on or from a disc, it is demanded for protecting the content that recording/playback operations be correctly controlled and unauthorized copying be prevented.

[0003]

For example, Patent Document 1 discloses that data is recorded or played back on or from discs by using a data format consisting of user data and user control data.

[0004]

In such a data format, the user data is recorded after being encrypted with a key by using the disc ID unique to a disc, thereby protecting content from unauthorized copying.

[0005]

Patent Document 2 discloses a recording/playback apparatus 1 shown in Fig. 1.

[0006]

In the example shown in Fig. 1, the recording/playback apparatus 1 is formed of a drive 11, an AV board 12, and a

dedicated bus 13. The drive 11 includes a recording/playback processor 21, and the AV board 12 includes an AV content processor 31, a content protector 32, an input unit 33, and an output unit 34.

[0007]

When an optical disc 41 is loaded, the recording/playback processor 21 obtains the disc ID and RKB (Renewal Key Block) unique to the optical disc 41, and supplies them to the content protector 32 of the AV board 12 via the dedicated bus 13. The content protector 32 generates a key by using a disc key obtained from the disc ID and RKB, and stores the generated key.

[0008]

The AV content processor 31 supplies content with a copyright (i.e., such content should be protected) received via the input unit 33, for example, an antenna, to the content protector 32. The content protector 32 encrypts the content with the prestored key by using the disc key obtained from the disc ID and RKB, and supplies the encrypted content to the recording/playback processor 21 via the dedicated bus 13 as the content to be protected. The recording/playback processor 21 receives the encrypted content and records it on the optical disc 41.

[0009]

The recording/playback processor 21 also plays back

predetermined encrypted content from the optical disc 41, and supplies the content to the content protector 32 via the dedicated bus 13. The content protector 32 decrypts the encrypted content with a key by using the disc key obtained from the disc ID and RKB, and supplies the content to the AV content processor 31. The AV content processor 31 decodes the decrypted content according to, for example, an MPEG (Moving Picture Experts Group) and plays back the content. The output unit 34 outputs the played back content.

[0010]

As described above, since data is sent and received between the drive 11 and the AV board 12 via the dedicated bus 13 in the recording/playback apparatus 1, content can be protected from external access by using the disc ID or RKB.

[0011]

As a modified example of the recording/playback apparatus 1 shown in Fig. 1, a recording/playback apparatus 51 shown in Fig. 2 can be considered. In Fig. 2, the elements corresponding to the elements shown in Fig. 1 are designated with like reference numerals, and an explanation thereof is thus omitted. In the example shown in Fig. 2, the drive 11 and the AV board 12 are separated via a bus 61 (general-purpose bus) (for example, they are separated by a household LAN (Local Area Network)).

[0012]

Accordingly, in the example shown in Fig. 2, since the disc ID and RKB are directly sent to the bus 61, there is a possibility of the disc ID and RKB being stolen. For example, when connecting an HDD (Hard Disk Drive) 71 to the bus 61 for recording content, the "disc ID", "RKB", and "content encrypted with a disc key obtained from the disc ID and the RKB" on the bus 61 are sent (monitored) and copied into the HDD 71.

[0013]

In the example shown in Fig. 2, in the HDD 71, a 16-B disc ID, a several-MB RKB, 20-GB encrypted content, and a several-KB program which are sent to the HDD 71 as described above are stored. If the "disc ID", "RKB", and "content encrypted with the disc key obtained from the disc ID and RKB" are supplied to the AV board 12 from the HDD 71, the AV board 12 disadvantageously plays back the content since it cannot distinguish them from those played back by the authorized optical disc 41.

[0014]

A "spoofing drive" or a "spoofing program", which supplies the "disc ID", "RKB", and "content encrypted with the disc key obtained from the disc ID and RKB" to the AV board 12 may be disadvantageously distributed as a general playback execution apparatus or program.

[0015]

Accordingly, in the recording/playback apparatus 51 in which the drive 11 and the AV board 12 are separated from each other via the bus 61, data may be distributed, not only to authorized discs, but also to unauthorized media, for example, the HDD 71.

[0016]

Accordingly, a recording/playback apparatus 81 which conducts mutual authentication, such as that shown in Fig. 3, has been proposed. In the example shown in Fig. 3, a mutual authentication unit 91 is provided for the drive 11, and a mutual authentication unit 92 is provided for the AV board 12. By conducting mutual authentication processing between the two mutual authentication units 91 and 92, content can be sent and received by being encrypted with a common key shared by the drive 11 and the AV board 12.

[0017]

Accordingly, in the HDD 71 without a mutual authentication function and compatible with optical discs recorded by the recording/playback 1 or 51, even if the "disc ID", "RKB", and "content encrypted with the disc key obtained from the disc ID and RKB" are copied, they cannot be decrypted, thereby making copying substantially impossible in the HDD 71. Thus, the above-described "spoofing drive" or "spoofing program" can be prevented.

[0018]

[Patent Document 1] Japanese Unexamined Patent
Application Publication (Translation of PCT Application) No.
2002-521789

[Patent Document 2] Japanese Unexamined Patent
Application Publication No. 2002-84271

[0019]

[Problems to be Solved by the Invention]

Recently, however, for superdistribution in which encrypted content is provided free of charge, or for storing content in a PC (Personal Computer), it is demanded that content that does not have to be protected can be recorded or played back without being encrypted on the bus 13 so as to allow the user to copy such content. On the other hand, it is also demanded that content that should be protected be prevented from being copied.

[0020]

At present, however, since the HDD 71 of an ordinary PC is not provided with a mutual authentication function, in the recording/playback apparatus 81, not only specific content to be protected, but also content that does not have to be protected but to be stored in a PC, cannot be copied.

[0021]

In view of the above background, it is an object of the present invention to flexibly protect content based on whether or not the content should be protected.

[0022]

[Means for Solving the Problems]

According to a recording system of the present invention, an input device includes determination means for determining whether input content is to be protected, and a recording apparatus includes recording means for recording on a recording medium, together with the content, protection information indicating whether the content is to be protected when being transmitted on the bus based on a determination result obtained by the determination means.

[0023]

The recording means may record the protection information in predetermined units of the content.

[0024]

The predetermined unit may be 2048 bytes.

[0025]

The recording apparatus may further include encryption means for encrypting the content by using an ID and a recording medium key of the recording medium when the determination means determines that the content is to be protected.

[0026]

The recording apparatus may further include encryption means for encrypting the content by using at least a recording medium key of the recording medium when the

determination means determines that the content is not to be protected.

[0027]

Each of the input device and the recording apparatus may further include authentication means for authenticating each other.

[0028]

The input device may further include first encryption means for encrypting the content before being sent to the bus when the determination means determines that the content is to be protected. The recording apparatus may further include second encryption means for encrypting the content before being recorded by the recording means when the determination means determines that the content is to be protected.

[0029]

The first encryption means may prohibit the content from being encrypted before being sent to the bus when the determination means determines that the content is not to be protected.

[0030]

According to a first recording method of the present invention, an input device determines whether input content is to be protected, and a recording apparatus records on a recording medium, together with the content, protection

information indicating whether the content is to be protected when being transmitted on the bus based on a determination result.

[0031]

A recording apparatus of the present invention includes: authentication means for conducting mutual authentication with another apparatus connected to the recording apparatus via a bus; decryption means for decrypting content encrypted with a first encryption method and supplied from the first apparatus via the bus; and recording means for recording on the recording medium, together with the content decrypted by the decryption means, protection information indicating that the content is to be protected when being transmitted on the bus.

[0032]

The recording apparatus may further include encryption means for encrypting the decrypted content with a second encryption method.

[0033]

The encryption means may encrypt the decrypted content by using an ID and a recording medium key of the recording medium.

[0034]

The recording means may record the content together with protection information indicating that the content is

not to be protected when being transmitted on the bus when the content supplied from the another apparatus via the bus is not encrypted with the first encryption method.

[0035]

A second recording method of the present invention includes: an authentication step of conducting mutual authentication with another apparatus connected to a recording apparatus via a bus; a decryption step of decrypting encrypted content supplied from the first apparatus via the bus; and a recording step of recording on a recording medium, together with the content decrypted by processing of the decryption step, protection information indicating that the content is to be protected when being transmitted on the bus.

[0036]

A program of a first recording medium of the present invention includes: an authentication step of conducting mutual authentication with another apparatus connected to a recording apparatus via a bus; a decryption step of decrypting encrypted content supplied from the another apparatus via the bus; and a recording step of recording on a recording medium, together with the content decrypted by processing of the decryption step, protection information indicating that the content is to be protected when being transmitted on the bus.

[0037]

A first program of the present invention includes: an authentication step of conducting mutual authentication with another apparatus connected to a recording apparatus via a bus; a decryption step of decrypting encrypted content supplied from the another apparatus via the bus; and a recording step of recording on a recording medium, together with the content decrypted by processing of the decryption step, protection information indicating that the content is to be protected when being transmitted on the bus.

[0038]

An input device of the present invention includes: authentication means for conducting mutual authentication with a recording apparatus connected to the input device via a bus; first encryption means for encrypting the content with a first encryption method according to whether the input content is to be protected when being transmitted on the bus; and supply means for supplying the content encrypted by the first encryption means to the recording apparatus via the bus.

[0039]

The input device may further include second encryption means for encrypting the content encrypted by the first encryption means with a second encryption method.

[0040]

One of the first encryption means and the second encryption means may encrypt the content by using an ID and a recording medium key of a recording medium.

[0041]

An input method of the present invention includes: an authentication step of conducting mutual authentication with a recording apparatus connected to an input device via a bus; an encryption step of encrypting content according to whether the input content is to be protected when being transmitted on the bus; and a supply step of supplying the content encrypted by processing of the encryption step to the recording apparatus via the bus.

[0042]

A program of a second recording medium of the present invention includes: an authentication step of conducting mutual authentication with a recording apparatus connected to an input device via a bus; an encryption step of encrypting content according to whether the input content is to be protected when being transmitted on the bus; and a supply step of supplying the content encrypted by processing of the encryption step to the recording apparatus via the bus.

[0043]

A second program of the present invention includes: an authentication step of conducting mutual authentication with

a recording apparatus connected to an input device via a bus; an encryption step of encrypting content according to whether the input content is to be protected when being transmitted on the bus; and a supply step of supplying the content encrypted by processing of the encryption step to the recording apparatus via the bus.

[0044]

A playback apparatus according to the present invention includes: playback means for playing back from a recording medium content and protection information indicating whether the content is to be protected when being transmitted on the bus; and output control means for controlling the output of the content to another apparatus via the bus on the bus based on the protection information played back by the playback means.

[0045]

The protection information may be recorded in predetermined units of the content.

[0046]

The predetermined unit may be 2048 bytes.

[0047]

The playback apparatus may further include: authentication means for authenticating the another apparatus; and encryption means for encrypting the content. The encryption means may encrypt the content before being

sent to the bus when the protection information indicates that the content is to be protected when being transmitted on the bus and when the another apparatus is authenticated by the authentication means.

[0048]

The output control means may prohibit the content from being output to the bus when the protection information indicates that the content is to be protected when being transmitted on the bus and when the another apparatus is not authenticated by the authentication means.

[0049]

A playback method of the present invention includes: a playback step of playing back from a recording medium content and protection information indicating whether the content is to be protected when being transmitted on the bus; and an output control step of controlling the output of the content to another apparatus via a bus based on the protection information played back by processing of the playback step.

[0050]

A program of a third recording medium of the present invention includes: a playback step of playing back from the recording medium content and protection information indicating whether the content is to be protected when being transmitted on the bus; and an output control step of

controlling the output of the content to another apparatus via a bus based on the protection information played back by processing of the playback step.

[0051]

A program of the present invention includes: a playback step of playing back from a recording medium content and protection information indicating whether the content is to be protected when being transmitted on the bus; and an output control step of controlling the output of the content to another apparatus via a bus based on the protection information played back by processing of the playback step.

[0052]

In the first invention, the input device determines whether input content is to be protected, and the recording apparatus records on a recording medium, together with the content, protection information indicating whether the content is to be protected when being transmitted on a bus based on a determination result.

[0053]

The input device may be an independent device, or may be a block for performing input processing in an input recording apparatus.

[0054]

The recording apparatus may be an independent apparatus, or may be a block for performing recording processing in a

recording/playback apparatus.

[0055]

In the second invention, mutual authentication is conducted with another apparatus connected via a bus. Encrypted content supplied from the another apparatus via the bus is then decrypted, and protection information indicating that the content is to be protected when being transmitted on the bus is recorded on a recording medium together with the decrypted content.

[0056]

In the third invention, mutual authentication is conducted with a recording apparatus connected via a bus. Content is then encrypted according to whether the input content is to be protected when being transmitted on the bus, and the encrypted content is supplied to the recording apparatus via the bus.

[0057]

In the fourth invention, content and protection information indicating whether the content is to be protected when being transmitted on a bus are played back from a recording medium. Based on the played back protection information, the output of the content to another apparatus on the bus is controlled.

[0058]

The playback apparatus may be an independent apparatus,

or may be a block for performing playback processing in a recording/playback apparatus.

[0059]

[Description of the Embodiments]

An embodiment of the present invention is described below with reference to the drawings.

[0060]

Fig. 4 illustrates an example of the configuration of a recording/playback apparatus 101 to which the present invention is applied. A drive 111, an AV board 112, and an HDD (hard disk drive) 114 are connected to a bus 113, a typical example of which is a household LAN (Local Area Network). It should be noted that the drive 111, the AV board 112, and the HDD 114 are separately sold, and these elements are then connected to the bus 113 by a user.

[0061]

In this example, the drive 111 and the AV board 112 are each provided with the corresponding private key and the public key. The public key and the private key have been registered when, for example, the drive 111 and the AV board 112 were shipped by manufacturers. The public key is stored in a digital signature issued by a certificate authority (not shown). Content is transferred between the drive 111 and the AV board 112 by using a public key cryptosystem, for example, RSA. Between the private key and the corresponding

public key, ciphertext generated based on one of the keys can be decrypted by using the other key.

[0062]

The drive 111 includes a mutual authentication unit 121 for conducting mutual authentication with other devices (the AV board 112 in the example shown in Fig. 4), an input/output controller 122 for controlling the elements of the drive 111, and a recording/playback processor 123 for recording or playing back content on or from an optical disc 141 loaded in the drive 111.

[0063]

The AV board 112 includes a mutual authentication unit 131 for conducting mutual authentication with other devices (the drive 111 in the example shown in Fig. 4), a content protector 132 for encrypting content to be stored in the optical disc 141, and an AV content processor 133 for receiving content via an input unit 134, for example, an antenna, or for decoding content and outputting it to an output unit 135.

[0064]

The mutual authentication unit 121 of the drive 111 conducts mutual authentication with the mutual authentication unit 131 of the AV board 112. More specifically, when the drive 111 and the AV board 112 are connected to turn on the power of the two devices, the

mutual authentication unit 131 of the AV board 112 generates a common key based on random numbers of a built-in random number generator (not shown) and encrypts the generated common key with the public key of the drive 111 so as to generate a signature to the common key encrypted with the private key of the AV board 112. The mutual authentication unit 131 reads an AV-board digital certificate that has been obtained from a certificate authority and stored in a built-in memory, and sends the encrypted common key, the signature added to the common key by the AV board 112, and the AV-board digital certificate to the drive 111 via the bus 113.

[0065]

Upon receiving the above-described elements, the mutual authentication unit 121 of the drive 111 decrypts the encrypted common key with the private key of the drive 111 to obtain the common key (first common key), and also decrypts the AV-board digital certificate with the public key of the certificate authority obtained from the certificate authority so as to verify that the AV board 112 is an authorized AV board. The mutual authentication unit 121 also decrypts the signature added to the common key with the public key of the AV board 112 obtained from the decrypted AV-board digital certificate so as to obtain the common key (second common key). The mutual authentication unit 121 of the drive 111 compares the first common key with

the second common key, and when they are found to be equal to each other, the mutual authentication unit 121 determines that the common key has not been tampered with on the bus 113. Then, the common key can be shared between the drive 111 and the AV board 112.

[0066]

As described above, the mutual authentication unit 121 of the drive 111 performs mutual authentication with the mutual authentication unit 131 of the AV board 112 so as to authenticate the AV board 112. Then, the mutual authentication units 121 and 131 can encrypt and send content, and decrypt the received content by using the common key.

[0067]

On the other hand, the HDD 114 does not have a mutual authentication function, such as the mutual authentication unit 131 of the AV board 112. Accordingly, the HDD 114 can send and receive free content (content that does not have to be protected), which can be transmitted to the bus 113 without any problem, to and from the drive 111.

[0068]

Upon receiving a broadcast signal (corresponding to encrypted or scrambled content) via the input unit 134, the AV content processor 133 of the AV board 112 decodes the encrypted or scrambled content with a prestored key (key

shared with a device which transmits the broadcast signal) and supplies the content to the content protector 132.

[0069]

The AV content processor 133 determines whether the input content should be protected based on whether or not the input content is encrypted or scrambled. If, for restricting the copying of the content, CCI (Copy Control Information), for example, a CGMS (Copy Generation Management System) signal, indicating "Copy Free (copying is allowed)", "Copy Once (copying is allowed only for one generation", "No More Copy (copying is not allowed further than this generation", or "Copy Prohibited (copying is not allowed)", is added to this content (broadcast signal), the above-described determination may be made as follows. When this copy generation management information indicates "Copy Free", the input content may be determined as content that does not have to be protected, and when the copy generation management information indicates "Copy Once", "No More Copy", or "Copy Prohibited", the input content may be determined as content that should be protected.

[0070]

If the content input from the AV content processor 133 is found to be content that should be protected by the AV content processor 133, the content protector 132 obtains the disc key by using the RKB of the optical disc 141 supplied

from the mutual authentication unit 131 so as to generate a block key based on the disc key and the disc ID of the optical disc 141. The content protector 132, by using the block key, encrypts the content which should be protected on the optical disc 141 and supplies the encrypted content to the encryption authentication unit 131.

[0071]

The mutual authentication unit 131 encrypts the content, which has been encrypted by the content protector 132, by using the common key shared with the drive 111 in order to protect the content on the bus 113, and outputs the encrypted content to the drive 111 via the bus 113.

[0072]

If the content is found to be content that does not have to be protected by the AV content processor 133, the content protector 132 and the mutual authentication unit 131 output the content to the drive 111 via the bus 113 without encrypting it.

[0073]

The mutual authentication unit 121 of the drive 111 receives the content from the AV board 112 via the bus 113. If the received content is encrypted, the mutual authentication unit 121 decrypts the content with the common key shared with the drive 111 and supplies the decrypted content to the recording/playback processor 123.

[0074]

The input/output controller 122 determines whether the content input into the mutual authentication unit 121 should be protected on the bus 113 based on whether the content is encrypted with the common key shared with the AV board 112 by the mutual authentication unit 131 of the AV board 112 (that is, whether the AV content processor 133 has determined whether the content should be protected). The input/output controller 122 then controls the recording of the content by the recording/playback processor 123 based on whether the input content should be protected on the bus 113 and whether the mutual authentication unit 121 has conducted mutual authentication with the AV board 112.

[0075]

The input/output controller 122 also controls the recording/playback processor 123 to play back disc information, such as the disc ID and RKB (Renewal Key Block), recorded on the optical disc 141 based on whether the input content should be protected and whether the mutual authentication unit 121 has conducted mutual authentication with the AV board 112.

[0076]

When recording the content on the optical disc 141, the recording/playback processor 123 generates protection information indicating whether or not the content to be

recorded should be protected on the bus 113 based on an instruction from the input/output controller 122, and records the protection information on the optical disc 141 together with the content.

[0077]

Fig. 5 illustrates an example of the configuration of a data format to be recorded on the optical disc 141.

[0078]

In this data format, user data 201 for 32 frames, each frame having 2K (2048) bytes, and user control data 202 for 32 frames, each frame having 18 bytes, so as to form 32 sectors.

[0079]

The user data 201 is formed of content data. In this user data 201, four (4-byte) EDCs (error detecting codes) are added to each frame so as to form a data frame 203 shown in Fig. 6.

[0080]

In the example shown in Fig. 6, one data frame has 2052 bytes. More specifically, one data frame consists of 2048 user data bytes having numbers Ud0 through Ud2047 and four EDCs having numbers ed2048 through ed2051.

[0081]

This data frame 203 forms a scramble data frame 205 shown in Fig. 7 based on a 16 × 9-byte physical address 204,

the scramble data 205 consisting of 32 data frames 203.

[0082]

In the example in Fig. 7, the first frame (the leftmost column in Fig. 7) has 2052 bytes having numbers $d(0, 0)$, $d(1, 0)$, ..., and $d(2051, 0)$. The second frame (the second column from the left in Fig. 7) has 2052 bytes having numbers $d(0, 1)$, $d(1, 1)$, ..., and $d(2051, 1)$. Similarly, the $(F-1)$ -th frame has 2052 bytes having numbers $d(0, F)$, $d(1, F)$, ..., and $d(2051, F)$, and the 32-th frame (the rightmost column in Fig. 7) has 2052 bytes having numbers $d(0, 31)$, $d(1, 31)$, ..., and $d(2051, 31)$.

[0083]

From the above-described scramble data frame 205, 216-row \times 304-column data block 206 is formed. By adding 32-row parity to the data block 206, an LDC (long distance code: error correction) block 207 is formed. From the LDC block 207, a 496-row \times 152-column LDC cluster 208 is formed. The LDC cluster 208 is divided into four LDC blocks, each having 38 columns, 209-1 through 209-4, which form an ECC cluster 221 with BIS blocks 213-1 through 213-3, which are described below.

[0084]

Addresses and control data to be added by this recording/playback apparatus 101 are as follows. The user control data (logical address and control data) 202 is

arranged as 32×18 bytes, as shown in Fig. 8.

[0085]

In the example shown in Fig. 8, the first (the leftmost column in Fig. 8) frame has 18 bytes having numbers $UC(0, 0)$, $UC(1, 0)$, ..., $UC(17, 0)$. The second (the second column from the left in Fig. 8) frame has 18 bytes having numbers $UC(0, 1)$, $UC(1, 1)$, ..., $UC(17, 1)$. Similarly, the $(S-1)$ -th frame has 18 bytes having numbers $UC(0, S)$, $UC(1, S)$, ..., $UC(17, S)$. The 32-th (the rightmost column in Fig. 8) frame has 2052 bytes having numbers $UC(0, 31)$, $UC(1, 31)$, ..., $UC(17, 31)$.

[0086]

As discussed above, in this data format, the 18-byte user control data 202 corresponds to the 2K(2048)-byte user data 201 in each frame. Accordingly, protection information indicating whether data (content) should be protected on the bus 113 is generated for the data (content) to be recorded in this user data 201 (2K bytes). This protection information is stored in the least significant bit of the first byte $UC(0, S)$ of the user control data 202 (18 bytes) corresponding to the user data 201.

[0087]

For example, if the content to be recorded is content that should be protected on the bus 113, "0" is generated and recorded in the least significant bit of the first byte

(0, S) of the user control data 202 (18 bytes) as the protection information. If the content to be recorded is content that does not have to be protected on the bus 113, "1" is generated and recorded in the least significant bit of the first byte UC(0, S) of the user control data 202 (18 bytes) as the protection information. In a known data format, "0" is stored in the least significant bit of the first byte UC(0, S) of the user control data 202 (18 bytes) (i.e., the least significant bit is unused). Accordingly, for content recorded in a known data format, information concerning content to be protected on the bus 113 is also stored, and thus, the data format used in this embodiment is compatible with the known data format.

[0088]

The protection information concerning content that should be protected may be set as "1", and the protection information concerning content that does not have to be protected may be set as "0". In this case, however, all items of known content should be content that does not have to be protected on the bus 113, and thus, they cannot be protected. Accordingly, it is preferable that the protection information concerning content that should be protected is set as "0", and the protection information concerning content that does not have to be protected is set as "1".

[0089]

The physical address 204 is arranged as 16×9 bytes. This physical address 204 indicates the physical distance on the disc 141.

[0090]

From the 32×18 -byte user control data 202, $24\text{-column} \times 30\text{-row}$ access block 210 is formed based on the physical address 204. 32-row parity is added to the access block 210 so as to form a BIS (burst instruction sub-code) block 211. The BIS block 211 is formed into a $3\text{-column} \times 496\text{-row}$ BIS cluster 212.

[0091]

The BIS cluster 212 fills the three BIS blocks 213-1 through 213-3 between the LDC blocks 209-1 through 209-4 so as to form the $155\text{-column} \times 496\text{-row}$ ECC cluster 221. From this ECC cluster 221, a physical cluster 222 consisting of 42 sets, each having 45 channel bit data (data) and one channel bit control data (dc contr.), is formed and is recorded on the optical disc 141.

[0092]

This physical cluster 222 is grouped into 496 recording frames having 1932 channel bits (1288 data bits). In the physical cluster 222, the 20 channel bits of the first data (data) are set as a synchronizing bit group (Frame Sync).

[0093]

As discussed above, when the content to be recorded is content that should be protected on the bus 113, the recording/playback processor 123 generates (stores) "0" as the protection information, and when the content to be recorded is content that does not have to be protected on the bus 113, the recording/playback processor 123 generates (stores) "1" as the protection information. The generated protection information is recorded in the user control data 202.

[0094]

To perform error correction for playing back the content of this data format recorded on the optical disc 141, BIS error correction is generally performed, and the result of BIS error correction is used as revocation information for conducting LDC error correction. Accordingly, since BIS error correction has been finished before outputting user data after LDC error correction, the user control data contained in the BIS has been obtained. Thus, the output of the user data can be controlled by using the user control data.

[0095]

When playing back the content recorded on the optical disc 141 by the recording/playback processor 123, the protection information recorded on the optical disc 141 is played back before the content. Thus, based on the played

back protection information, the input/output controller 122 controls the output of the content to the bus 113.

[0096]

For example, the input/output controller 122 controls the output of the content to the bus 113 by the mutual authentication unit 121 based on whether the mutual authentication unit 121 has conducted mutual authentication with the AV board 112 and whether the played back content is content to be protected on the bus 113 (whether the protection information is "0"). Based on the control of the input/output controller 122, the mutual authentication unit 121 encrypts the played back content with the common key shared with the drive 111, and outputs the content to the AV board 112 via the bus 113.

[0097]

Upon receiving the encrypted content from the mutual authentication unit 121 of the drive 111, the mutual authentication unit 131 of the AV board 112 decrypts the content and supplies it to the content protector 132.

[0098]

The content protector 132 further decrypts the content, which has been decrypted with the common key shared with the AV board 112 by the mutual authentication unit 131, by using the block key generated from the disc ID and the disc key of the optical disc 141, and supplies the decrypted content to

the AV content processor 133. The AV content processor 133 decodes the decrypted content according to, for example, an MPEG (Moving Picture Experts Group) and plays back the content. The output unit 135 outputs the played back content.

[0099]

As described above, since the AV board 112 conducts mutual authentication with the drive 111, content to be protected by a copyright or content that does not have to be protected can be sent and received between the AV board 112 and the drive 111.

[0100]

Even if, for example, content that should be protected is sent to the drive 111 from the HDD 114, mutual authentication is not conducted for the HDD 114 by the drive 111. If the content does not have to be protected, it is processed in the drive 111. That is, in this recording/playback apparatus 101, only copy free data without the need for mutual authentication can be recorded.

[0101]

As described above, in this recording/playback apparatus 101, the encryption of content or the output of content to a general-purpose bus is flexibly controlled according to whether content should be protected by a copyright.

[0102]

Fig. 9 illustrates an example of the configuration of the content protector 132. In Fig. 9, only the content protector 132 and the optical disc 141 are shown for the sake of convenience. In actuality, however, as shown in Fig. 4, the mutual authentication unit 131, the bus 113, the mutual authentication unit 121, and the recording/playback processor 123 perform the corresponding processing between the content protector 132 and the optical disc 141.

[0103]

In the example in Fig. 9, the content protector 132 is formed of an RKB processor 252, a key generator 253, and an encryption unit 254.

[0104]

The RKB processor 252 obtains a disc key by using the RKB supplied from the optical disc 141, and the device ID and the device key stored in the content protector 132 based on whether the content received from the AV content processor 133 is content that should be protected (the processing for obtaining the disc key is disclosed in Patent Document 2 and is described in detail below with reference to Figs. 10 through 12).

[0105]

The key generator 253 generates a block key by using the disc key obtained by the RKB processor 252, the disc ID

supplied from the optical disc 141, and recording information stored in the content protector 132 (for example, information used when recording, such as a block seed, a title key, or a recording mode).

[0106]

If the content supplied from the optical disc 141 is encrypted, the encryption unit 254 decrypts the encrypted content by using the block key generated by the key generator 253, and outputs the content to the AV content processor 133. If the content supplied from the optical disc 141 is not encrypted, the encryption unit 254 directly outputs the content to the AV content processor 133.

[0107]

If the content supplied from the AV content processor 133 is found to be the content to be protected based on information indicating whether the content received from the AV content processor 133 is content to be protected, the encryption unit 254 encrypts the content by using the block key generated by the key generator 253 in order to protect the content on the optical disc 141, and outputs the content to the optical disc 141. If the content supplied from the AV content processor 133 is content that does not have to be protected, the encryption unit 254 directly (without encrypting the content) supplies the content to the optical disc 141.

[0108]

Details of the RKB used for the disc-key obtaining processing are given below. Fig. 10 illustrates a structure in which keys are distributed to the recording/playback apparatus 101 of the present invention. Numbers 0 through 15 indicated at the bottommost line of Fig. 10 correspond to the individual recording/playback apparatuses (devices). That is, leaves in the tree structure shown in Fig. 10 correspond to the recording/playback apparatuses.

[0109]

Device 0 through device 15 each store, in the initial tree which was set when the devices were manufactured (shipped), the keys (node keys) assigned to the nodes from the device leaf to the root (topmost level) and the leaf key of the corresponding leaf. K0000 through K1111 indicated at the bottommost level in Fig. 10 are leaf keys assigned to device 0 through device 15, respectively, and keys KR through K111 from KR positioned at the topmost level to the nodes positioned at the second level from the bottommost level are node keys.

[0110]

In the example in Fig. 10, for example, device 0 owns leaf key K0000, and node keys K000, K00, K0, and KR. Device 5 owns K0101, K010, K01, K0, and KR. Device 15 owns K1111, K111, K11, K1, and KR. In the tree shown in Fig. 10, only

16 devices are shown, and the tree structure, which consists of four levels, is vertically symmetrical with each other. However, more devices may be formed in the tree, or the number of levels may be different at each portion of the tree.

[0111]

The recording/playback apparatuses contained in the tree structure shown in Fig. 10 use various recording media, for example, DVD, CD, MD (trademark), Memory Stick®. It is also assumed that various application services coexist in the tree structure. The key distribution structure shown in Fig. 10 is applied to a system in which different devices and different applications coexist.

[0112]

In a system in which various devices and applications coexist, for example, the portion surrounded by the broken line in Fig. 10, i.e., devices 0, 1, 2, and 3 are set as one group using the same recording medium. In this tree structure, the four devices 0, 1, 2, and 3 contained in the same group own common keys K00, K0, and KR as node keys. By utilizing this configuration in which the same node keys are shared, for example, a common master key can be provided only to the devices 0, 1, 2, and 3.

[0113]

If, for example, the node key K00 itself shared by the

devices 0, 1, 2, and 3 is set as the master key, the master key, which is common only for the devices 0, 1, 2, and 3, can be set without sending a new key. Alternatively, a value $\text{Enc}(K00, K_{\text{master}})$ generated by encrypting a new master key K_{master} with the node key $K00$ is distributed to the devices 0, 1, 2, and 3 via a network or by storing the value in the recording medium, and then, only the devices 0, 1, 2, and 3 can obtain the master key K_{master} by decrypting the encryption $\text{Enc}(K00, K_{\text{master}})$ with the common node key $K00$ shared by the devices. $\text{Enc}(K_a, K_b)$ indicates that K_b is encrypted with K_a .

[0114]

If, at a certain time t , the keys $K0011$, $K001$, $K00$, $K0$, and KR owned by device 3 are decrypted and disclosed by an attacker (hacker), it is necessary to disconnect device 3 for protecting data to be sent and received in the system (the group of devices 0, 1, 2, and 3). Accordingly, the node keys $K001$, $K00$, $K0$, and KR are changed to new keys: $K(t)001$, $K(t)00$, $K(t)0$, $K(t)R$, respectively, and these renewal keys should be reported to devices 0, 1, and 2. $K(t)aaa$ indicates that this is a renewal key of the key $Kaaa$ at a generation t .

[0115]

Distribution processing for renewal keys is as follows. Keys are renewed by supplying a table consisting of block

data, which is referred to as "RKB (Renewal Key Block)", such as that shown in Fig. 11A, to devices 0, 1, and 2 via a network or by storing the table in a recording medium.

[0116]

The RKB shown in Fig. 11A is formed as block data having a data configuration that enables only the corresponding devices to renew the node keys. Fig. 11 illustrates an example of block data for distributing the renewal node keys at a generation t to devices 0, 1, and 2 in the tree structure shown in Fig. 10. As described above, device 0 and device 1 need $K(t)00$, $K(t)0$, and $K(t)R$ as the renewal node keys, and device 2 needs $K(t)001$, $K(t)00$, $K(t)0$, and $K(t)R$ as the renewal node keys.

[0117]

The RKB contains a plurality of encrypted keys, such as those in the RKB shown in Fig. 11A. The encrypted key in the bottommost line is $\text{Enc}(K0010, K(t)001)$, which is the renewal node key $K(t)001$ encrypted with the leaf key $K0010$ owned by device 2. Device 2 decrypts this encrypted key with the leaf key owned by device 2 so as to obtain $K(t)001$. By using decrypted $K(t)001$, the encrypted key $\text{Enc}(K(t)001, K(t)00)$ in the second line from the bottom in Fig. 11A can be decrypted so as to obtain the renewal node key $K(t)00$. Thereafter, the encrypted key $\text{Enc}(K(t)00, K(t)0)$ in the second line from the top in Fig. 11A is decrypted so as to

obtain the renewal node key $K(t)0$, and then, the encrypted key $\text{Enc}(K(t)0, K(t)R)$ in the topmost line in Fig. 11A is decrypted to obtain $K(t)R$.

[0118]

The node key $K000$ is not a key which should be renewed. The renewal node keys required by devices 0 and 1 are $K(t)00$, $K(t)0$, and $K(t)R$. Thus, device 0 and device 1 decrypt the encrypted key $\text{Enc}(K000, K(t)00)$ in the third line from the top in Fig. 11A so as to obtain $K(t)00$. Then, device 0 and device 1 decrypt the encrypted key $\text{Enc}(K(t)00, K(t)0)$ in the second line from the top in Fig. 11A so as to obtain the renewal node key $K(t)0$, and further decrypt the encrypted key $\text{Enc}(K(t)0, K(t)R)$ in the topmost line in Fig. 11A so as to obtain $K(t)R$. In this manner, devices 0, 1, and 2 can obtain the renewal key $K(t)R$. The index in Fig. 11A indicates the absolute addresses of the node keys and leaf keys used as decryption keys.

[0119]

If only the node key $K00$ is required to be renewed without the need to renew the node keys $K0$ and KR at the top two levels in the tree structure in Fig. 10, the RKB shown in Fig. 11B can be used for distributing the renewal node keys $K(t)00$ to devices 0, 1, and 2.

[0120]

The RKB shown in Fig. 11B can be used, for example,

when distributing a new master key shared in a specific group. It is now assumed, for example, that devices 0, 1, 2, and 3 in the group surrounded by the broken line of Fig. 10 use a recording medium and require a new common master key $K(t)_{\text{master}}$. In this case, data $\text{Enc}(K(t), K(t)_{\text{master}})$ generated by encrypting the new common renewal master key $K(t)_{\text{master}}$ with $K(t)_{00}$ renewed from the node key K_{00} shared between devices 0, 1, 2, and 3 is distributed together with the RKB shown in Fig. 11B. Accordingly, the data is not decrypted in the devices of another group, for example, device 4.

[0121]

Devices 0, 1, 2, and 3 can decrypt the above-described ciphertext by using $K(t)_{00}$ obtained by processing the RKB so as to obtain the master key $K(t)_{\text{master}}$ at a generation t .

[0122]

In the above-described example, the master key is transmitted to each recording/playback apparatus by using the RKB, and the recording/playback apparatus records and plays back data by using the master key. In the present invention, however, the disc key restricted for recording media is used as the above-described master key. This disc key is generated, as shown in Fig. 12, by using the RKB (Renewal Key Block) of the recording medium. The disc key $K(t)_{\text{media}}$ is a master key restricted only for recording

media, and the basic configuration is similar to that of the master key, and thus, an explanation thereof is omitted.

[0123]

In the example shown in Fig. 12, device 0 generates the renewal node key $K(t)00$ by using the RKB at a generation t stored in the recording medium, the leaf key $K0000$ stored in device 0, and the node keys $K000$ and $K00$ so as to obtain the renewal disc key $K(t)media$. The obtained $K(t)media$ is used for recording and playing back data on and from the recording medium.

[0124]

The pre-recording generation number (Generation #n) in Fig. 12 is not essential and is set as an option since the concept of old and new generations used in the master key does not exist in the disc key.

[0125]

As described above, the disc key is obtained based on the RKB from the optical disc 141, the device ID (for example, device 0 in Fig. 10) from the content protector 132, the device key (for example, leaf key $K0000$ of device 0 in Fig. 10), and node keys (for example, $K000$, $K00$, and so on, in device 0 in Fig. 10). This disc-key obtaining processing may be performed when the optical disc 141 is loaded in the drive 111 of the recording/playback apparatus 101 for recording or playing back content. Alternatively, the disc-

key obtaining processing may be performed when an instruction to record or play back content is given after the optical disc 141 is installed.

[0126]

A description is now given of mutual authentication processing performed by the AV board 112 of the recording/playback apparatus 101 with reference to the flowchart of Fig. 13.

[0127]

When the drive 111 and the AV board 112 are connected to turn on the power of the two elements, in step S11, the mutual authentication unit 131 of the AV board 112 generates a common key based on random numbers in a built-in random number generator. In step S12, the mutual authentication unit 131 encrypts the generated common key with the public key of the drive 111. In step S13, the mutual authentication unit 131 generates a signature to the common key encrypted with the private key of the AV board 112. In step S14, the mutual authentication unit 131 reads an AV-board digital certificate which has been obtained from a certificate authority (not shown) and stored in a built-in memory. In step S15, the mutual authentication unit 131 sends the encrypted common key, the signature added to the common key by the AV board 112, and the AV-board digital certificate to the drive 111 via the bus 113.

[0128]

In this manner, the encrypted common key, the signature to the common key by the AV board 112, and the AV-board digital certificate are sent to the drive 111 from the AV board 112. Mutual authentication processing performed by the drive 111 corresponding to the mutual authentication processing by the AV board 112 is described below with reference to the flowchart of Fig. 14.

[0129]

In step S31, the mutual authentication unit 121 of the drive 111 decrypts the received AV-board digital certificate based on the public key of the certificate authority, which has been obtained or is obtained when necessary. In step S32, the mutual authentication unit 121 determines whether the AV board 112 is an authorized AV board based on the AV-board digital certificate decrypted in step S31. If the AV-board digital certificate cannot be decrypted or is tampered with, it is determined in step S32 that the AV board 12 is not an authorized AV board, and the processing is terminated.

[0130]

If it is determined in step S32 that the AV board 112 is an authorized AV board, the AV-board digital certificate is decrypted to obtain the public key of the AV board 112. In step S33, the mutual authentication unit 121 decrypts the encrypted common key with the private key of the drive 111.

In step S34, the mutual authentication unit 121 decrypts the signature to the common key added by the AV board 112 by using the public key of the AV board 112.

[0131]

In step S35, the mutual authentication unit 121 compares the common key decrypted in step S33 with the plaintext common key provided with the signature, and determines whether the two common keys coincide with each other. Accordingly, the mutual authentication unit 121 determines whether the common key is an authorized common key. If it is determined in step S35 that the common key matches the common key provided with the signature, the mutual authentication unit 121 determines that the authorized common key has been received from the AV board 112. Then, in step S36, the mutual authentication unit 121 stores the common key. In contrast, if it is found in step S35 that the common key does not coincide with the common key provided with the signature, the mutual authentication unit 121 determines that the common key has been tampered with between the AV board 112 and the drive 111, and terminates the processing.

[0132]

Mutual authentication has been conducted between the drive 111 and the AV board 112 as described above, and processing thereafter is executed by sharing the common key

between the drive 111 and the AV board 112.

[0133]

Although an explanation is not given, the mutual authentication unit 121 of the drive 111 may further encrypt the common key obtained from the AV board 112 by using the public key of the drive 111, and send the encrypted common key, a signature to the encrypted common key added by the drive 111, and a drive digital certificate to the AV board 112, and request the AV board 112 to authenticate them.

[0134]

Recording request processing performed by the AV board 112 of the recording/playback apparatus 101 is described below with reference to the flowchart of Fig. 15.

[0135]

In step S101, the AV content processor 133 waits until content is input. Upon receiving a broadcast signal (signal corresponding to content) via the input unit 134, for example, an antenna, the AV content processor 133 determines in step S101 that content has been input. Then, in step S102, the AV content processor 133 determines whether the input content should be protected based on whether or not the input content is encrypted or scrambled.

[0136]

If it is determined in step S102 that the content should be protected, the AV content processor 133 decrypts

the encrypted or scrambled content by a prestored key (key shared with a device which transmits the broadcast signal). In step S103, the AV content processor 133 controls the control protector 132 to generate a block key. The block-key generation processing is described below with reference to the flowchart of Fig. 16. A description is also given, with reference to the flowchart of Fig. 17, of drive information obtaining processing performed by the drive 111 corresponding to the block-key generation processing by the AV board 112 shown in Fig. 16.

[0137]

In step S121, the RKB processor 252 outputs a request to read disc information (for example, the disc ID and RKB) of the optical disc 141 to the drive 111. More specifically, the RKB processor 252 outputs a request to read the disc ID and RKB of the optical disc 141 to the mutual authentication unit 131. The mutual authentication unit 131 outputs a request to read the disc ID and RKB to the mutual authentication unit 121 of the drive 111 via the bus 113.

[0138]

In step S141, the mutual authentication unit 121 of the drive 111 receives a request to read the disc ID and RKB of the optical disc 141 from the AV board 112 via the bus 113.

[0139]

In step S142, the input/output controller 122

determines based on the information from the mutual authentication unit 121 whether the AV board 112, which has sent a request to read the disc ID and RKB, has been mutually authenticated by the drive 111. If it is determined in step S142 that the AV board 112 has not been mutually authenticated by the drive 111, the disc-information playback processing by the drive 111 is terminated. Accordingly, requests from unauthorized devices can be rejected.

[0140]

As described above, since the AV board 112 has been mutually authenticated by the drive 111, it is determined in step S142 that the AV board 112 has been mutually authenticated by the drive 111. In this case, in step 143, the recording/playback processor 123 plays back the disc ID and RKB recorded on the optical disc 141 and supply them to the mutual authentication unit 121.

[0141]

In step S144, the mutual authentication unit 121 encrypts the disc ID and RKB supplied from the recording/playback processor 123 by using the common key shared with the AV board 112, and outputs the encrypted disc ID and RKB to the AV board 112 via the bus 113.

[0142]

In step S122, upon receiving the encrypted disc ID and

RKB via the bus 113, the mutual authentication unit 131 of the AV board 112 decrypts the disc ID and RKB with the common key shared with the drive 111, and supplies them to the RKB processor 251.

[0143]

In step S123, the RKB processor 251 obtains the disc key by using the supplied RKB, and the device ID and device key stored in a built-in memory. More specifically, the RKB processor 251 calculates the key $K(t)00$ of the node 00 at a time of pre-recording generation information (Generation #n) (for example, at time t in Fig. 12) by using the supplied RKB, the device ID (for example, device 0 in Fig. 10) and the device key (for example, leaf key $K0000$ of device 0 in Fig. 10) stored in the built-in memory, and the node keys (for example, $K000$, $K00$, $K0$, and KR of device 0 in Fig. 10). The RKB processor 251 then obtains ciphertext $\text{Enc}(K(t)00, K(t)\text{media})$, which is generated by encrypting the disc key $K(t)\text{media}$ with the key $K(t)00$, from the supplied RKB, and decrypts this ciphertext so as to obtain the disc key $K(t)\text{media}$.

[0144]

In step S124, the key generator 253 generates a block key by using the disc ID supplied from the mutual authentication unit 131, the disc key obtained in step S123, and recording information of the content protector 132, and

stores the block key in a built-in memory of the encryption unit 254.

[0145]

The block key is generated as described above, and in step S104 of Fig. 15, the encryption unit 254 encrypts the content supplied from the AV content processor 133 with the block key generated in step S124, and outputs the encrypted content to the mutual authentication unit 131.

[0146]

In step S105, the mutual authentication unit 131 further encrypts the content, which has been encrypted with the block key in step S104, by using the common key shared with the drive 111. In step S106, the mutual authentication unit 131 then outputs the encrypted content to the drive 111 via the bus 113.

[0147]

If it is determined in step S102 that the content received from the AV content processor 133 does not have to be protected, it is not necessary that the content be encrypted in the encryption unit 254 (to be protected on the optical disc 141) and be encrypted in the mutual authentication unit 131 (to be protected on the bus 113). Accordingly, steps S103 through S105 are skipped. That is, the encryption unit 254 outputs the content to the mutual authentication unit 131 without encrypting it (as the raw

data). In step S106, the mutual authentication unit 131 outputs the unencrypted content to the drive 111 via the bus 113.

[0148]

As discussed above, content to be protected is encrypted by using the block key obtained from the RKB and disc ID in the AV board 112. The content to be protected is further encrypted temporarily with the common key shared with the drive 111 and is output to the bus 113. In contrast, content that does not have to be protected is output to the bus 113 as the raw data. The recording processing performed by the drive 111 corresponding to the above-described processing is described below with reference to the flowchart of Fig. 18.

[0149]

In step S161, the mutual authentication unit 121 of the drive 111 receives the content from the AV board 112 via the bus 113.

[0150]

In step S162, the input/output controller 122 determines based on information supplied from the mutual authentication unit 121 whether the device which has sent the content has been mutually authenticated by the drive 111. If it is determined in step S162 that the AV board 112 has been mutually authenticated by the drive 111, the process

proceeds to step S163. In step S163, the input/output controller 122 determines whether the recording command of the input content is for content that should be protected on the bus 113 based on whether the content input into the mutual authentication unit 121 has been encrypted with the common key.

[0151]

If it is determined in step S163 that the recording command of this content is for content that should be protected on the bus 113, in step S164, the input/output controller 122 controls the mutual authentication unit 121 to decrypt the received content with the common key shared with the AV board 112. Accordingly, at this stage, this content is encrypted only with the block key obtained from the disc ID and RKB.

[0152]

In step S165, the input/output controller 122 controls the recording/playback processor 123 to generate protection information "0", which indicates that this content should be protected on the bus 113, and to store the protection information in the user control data UC(0, S) corresponding to this content. In step S168, the input/output controller 122 then records the protection information with the content encrypted with the block key on the optical disc 141.

[0153]

On the other hand, for example, content stored in the HDD 114 without a mutual authentication unit is input. In this case, in step S161, the mutual authentication unit 121 receives the content from the HDD 114 via the bus 113. Since the HDD 114 is not provided with a mutual authentication unit, it is determined in step S162 that the device which has sent the content has not been mutually authenticated by the drive 111, and the process proceeds to step S166. In step S166, the input/output controller 122 determines whether the recording command of the input content is for content that should be protected on the bus 113 based on whether the content input into the mutual authentication unit 121 has been encrypted with the common key.

[0154]

If it is determined in step S163 or S166 that the recording command of the input content is for content that does not have to be protected on the bus 113, the process proceeds to step S167. In step S167, the input/output controller 122 controls the recording/playback processor 123 to generate (store) protection information "1", which indicates that this content does not have to be protected on the bus 113, in the user control data UC(0, S) corresponding to this content. In step S168, the input/output controller 122 then records the generated protection information on the

optical disc 141 together with the unencrypted content.

[0155]

If it is determined in step S166 that the recording command of the input content is for content that should be protected on the bus 113, an error occurs, and the recording processing by the drive 111 is forcefully terminated.

Accordingly, in the drive 111, content from the unauthenticated HDD 114 is not recorded as the content that should be protected.

[0156]

As discussed above, content to be protected supplied from the authenticated AV board 112 is recorded on the optical disc 141 together with the protection information "0", which indicates that this content should be protected on the bus 113. In this case, the content to be protected is encrypted with the block key obtained from the disc ID and RKB. In contrast, content which does not have to be protected from the authenticated AV board 112 or content which does not have to be protected from the unauthenticated HDD 114 is stored in the optical disc 141 together with the protection information "1", which indicates that this content does not have to be protected on the bus 113. In this case, content that does not have to be protected has not been encrypted.

[0157]

The protection information stored as described above is played back by content playback processing by the drive 111, which is described below, and is used. The content playback processing by the drive 111 is described below with reference to the flowchart of Fig. 19.

[0158]

To output content recorded on the optical disc 141 which should be protected from the output unit 135 of the AV board 112, the user inputs a content playback command into the AV board 112 via an operation input unit (not shown). The mutual authentication unit 131 of the AV board 112 sends the playback command to the drive 111 via the bus 113. Accordingly, in step S191, the mutual authentication unit 121 receives the playback command from the AV board 112.

[0159]

In step S192, the input/output controller 122 determines whether the device to output the content (in this case, the AV board 112) has been mutually authenticated by the drive 111 based on the information from the mutual authentication unit 121. If it is determined in step S192 that the AV board 112 has been mutually authenticated, the input/output controller 122 determines in step S193 whether the playback command from the AV board 112 is for content to be protected.

[0160]

If it is determined in step S193 that the playback command from the AV board 112 is for content to be protected, in step S194, the recording/playback processor 123 plays back the specified content from the optical disc 141.

[0161]

As described with reference to Fig. 5, when playing back content, the protection information (user control data) recorded on the optical disc 141 is played back before the content. Accordingly, the input/output controller 122 determines in step S195 whether the user control data UC(0, S) corresponding to the content indicates "0". If UC(0, S) corresponding to the content is found to be "0", it means that this content should be protected on the bus 113. Then, in step S196, the input/output controller 122 controls the mutual authentication unit 121 to encrypt the played back content by using the common key shared with the AV board 112, and outputs the encrypted content to the AV board 112 via the bus 113. Accordingly, authorized data can be prevented from being obtained (hacked) on the bus 113.

[0162]

If it is determined in step S195 that UC(0, S) corresponding to the content is not "0" (UC(0, S) corresponding to the content is "1"), this content does not have to be protected on the bus 113, which is inconsistent with the playback command indicating that content should be

protected, supplied from the AV board 112. Thus, the playback processing by the drive 111 is terminated.

[0163]

On the other hand, in order to store (record) in the HDD 114 content recorded on the optical disc 141 that does not have to be protected, the user inputs a content playback command into the HDD 114 via an operation input unit (not shown). The HDD 114 sends the playback command to the drive 111 via the bus 113. Accordingly, in step S191, the mutual authentication unit 121 receives the playback command from the HDD 114.

[0164]

In step S192, the input/output controller 122 determines that the device to output the content (in this case, the HDD 114) has not been mutually authenticated based on the information from the mutual authentication unit 121. In this case, in step S197, the input/output controller 122 determines whether the playback command from the HDD 114 is for content to be protected.

[0165]

If it is determined in step S193 or S197 that the playback command from the device to output the content is for content that does not have to be protected, in step S198, the recording/playback processor 123 plays back the specified content from the optical disc 141. In step S199,

the input/output controller 122 determines whether UC(0, S) of the user control data associated with the content is "1". If UC(0, S) associated with the content is found to be "1", it means that this content does not have to be protected on the bus 113, and the process proceeds to step S200. In step S200, the input/output controller 122 controls the mutual authentication unit 121 to directly output the played back content (as the raw data) to the device to output the content (in this case, the AV board 112 or the HDD 114) via the bus 113.

[0166]

If it is determined in step S197 that the command from the HDD 114 is a playback command for content to be protected, or if it is determined in step S199 that UC(0, S) associated with the content is not "1" (UC(0, S) associated with the content is "0"), an error occurs since content to be protected cannot be output to the unauthenticated HDD 114. Thus, the output processing by the drive 111 is forcefully terminated. That is, in the drive 111, a playback command for the content to be protected supplied from the HDD 114 is rejected. Even if the command is a playback command for content that does not have to be protected, the corresponding content is not output if it is found that the command is for content to be protected on the bus 113.

[0167]

As discussed above, in response to the playback command from the authenticated AV board 112, the content to be protected on the bus 113 is encrypted with the common key and is output to the AV board 112 via the bus 113. The content that does not have to be protected on the bus 113 is directly output (without being encrypted) to the AV board 112 via the bus 113. Then, the content is received by the mutual authentication unit 131 of the AV board 112 in step S201 of Fig. 20, which is described below.

[0168]

In response to the playback command from the unauthenticated HDD 114, content to be protected on the bus 113 is not output. In contrast, content that does not have to be protected on the bus 113 is directly output (without being encrypted) to the HDD 114 via the bus 113. This enables the HDD 114 to store content that does not have to be protected. Thus, storage devices can be efficiently utilized.

[0169]

The content to be protected is encrypted with both the block key obtained from the disc ID and RKB and the common key which is authenticated between devices to send and receive the content (in this case, the drive 111 and the AV board 112). Accordingly, the content can be protected from unauthorized copying via the general-purpose bus 113.

[0170]

In a known recording/playback apparatus, "0" is stored in the least significant bit of the first byte UC(0, S) of the user control data 202 (18 bytes) corresponding to the content recorded on an optical disc which should be protected. Accordingly, the above-described playback processing for the content to be protected can be executed for content to be protected recorded in a known data format (for authenticated devices, content is encrypted with a common key and is output, and for unauthenticated devices, content is not output). Thus, content can be protected from unauthorized copying on the general-purpose bus 113. That is, the compatibility with known recording/playback apparatuses can be maintained.

[0171]

Playback processing by the AV board 112 associated with the above-described playback processing by the drive 111 is described below with reference to the flowchart of Fig. 20.

[0172]

The drive 111 receives the playback command for content to be protected from the AV board 112, plays back the content from the optical disc 141, and outputs the content via the bus 113. Thus, in step S201, the mutual authentication unit 131 of the AV board 112 receives the content. In step S202, the mutual authentication unit 131

of the AV board 112 then determines whether the received content is encrypted by the mutual authentication unit 121 of the drive 111 (whether the content is to be protected).

[0173]

If it is determined in step S202 that the content is encrypted with the common key, i.e., the content should be protected, in step S203, the mutual authentication unit 131 decrypts the received content with the common key shared with the drive 111, and outputs the content to the content protector 132. At this stage, this content is encrypted only with the block key obtained from the disc ID and RKB.

[0174]

In step S204, the content protector 132 performs block-key generation processing. This block-key generation processing is similar to that discussed with reference to Fig. 16, and thus, an explanation thereof is omitted. Simply, in step S204, the disc key is obtained from the RKB of the optical disc 141 so as to generate the disc key and the disc ID of the optical disc 141. Then, in step S205, the encryption unit 254 decrypts the content supplied from the mutual authentication unit 131 with the block key and supplies the encrypted content to the AV content processor 133.

[0175]

If it is determined in step S202 that the received

content is not encrypted, i.e., the content does not have to be protected, it is not necessary to decrypt this content. Accordingly, since the content passes through the mutual authentication unit 131 and the content protector 132, steps S203 through S205 are skipped.

[0176]

In step S206, the AV content processor 133 decodes the content supplied from the content protector 132 according to, for example, an MPEG (Moving Picture Experts Group) method, and plays it back. In step S207, the output unit 135 outputs the played back content.

[0177]

As discussed above, both the content to be protected and the content that does not have to be protected recorded on the optical disc 141 can be output to the AV board 112 which is mutually authenticated with the drive 111.

[0178]

In the above description, the AV board 112 generates a block key when recording or playing back the content after determining that the received content should be protected. However, this block-key generation processing may be performed by the content protector 132 of the AV board 112 every time the optical disc 141 is loaded.

[0179]

Fig. 21 illustrates another example of the

configuration of the recording/playback apparatus of the present invention. The basic configuration of a recording/playback apparatus 301 shown in Fig. 21 is similar to the recording/playback apparatus 101 shown in Fig. 4. In the recording/playback apparatus 301 shown in Fig. 21, however, the mutual authentication unit 121 of the drive 111 in the recording/playback apparatus 101 shown in Fig. 4 is removed.

[0180]

Thus, in the recording/playback apparatus 301 shown in Fig. 21, even though the AV board 112 is connected to the bus 113, it does not authenticated (a common key is not shared) by the AV board 112 since the drive 111 does not provided with a mutual authentication function. Accordingly, although content-playback-request processing from the AV board 112 is not executed in the drive 111, the drive 111 can send and receive content that does not have to be protected to and from the HDD 114 which is not provided with a mutual authentication function.

[0181]

Recording processing by the drive 111 of the recording/playback apparatus 301 is described below with reference to the flowchart of Fig. 22. Steps S211 through S214 of Fig. 22 are similar to step S161 and steps S166 through S168 of Fig. 18, and thus, a detailed explanation

thereof is omitted to avoid repeated explanations.

[0182]

In step S211, content that does not have to be protected is received from the HDD 114 by the recording/playback processor 123 via the bus 113. In step S212, the input/output controller 122 determines that the recording command is not for content to be protected on the bus 113 since the content input into the mutual authentication unit 121 is not encrypted with a common key. In step S213, the recording/playback processor 123 generates and stores the protection information "1", which indicates that this content does not have to be protected on the bus 113, in the user control data UC(0, S) associated with the content. Then, in step S214, the recording/playback processor 123 records this content that does not have to be protected from the HDD 114 on the optical disc 141.

[0183]

If it is determined in step S212 that content encrypted with a common key is input and that the recording command is for content to be protected, an error occurs, and the recording processing by the drive 111 is forcefully terminated.

[0184]

In this manner, content from the HDD 114 without a mutual authentication function can be recorded on the

optical disc 141 together with protection information indicating that this content does not have to be protected on the bus 113.

[0185]

Playback processing by the drive 111 of this recording/playback apparatus 301 is described below with reference to the flowchart of Fig. 23. Steps S221 through S225 of Fig. 23 are similar to step S191 and steps S197 through S200 of Fig. 19, and a detailed explanation thereof is thus omitted to avoid repeated explanations.

[0186]

For example, in order to store (record) in the HDD 114 content recorded on the optical disc 141 that does not have to be protected, the user inputs a content playback command into the HDD 114 via the input unit 617. The HDD 114 sends the playback command to the drive 111 via the bus 113. In step S221, the playback command from the HDD 114 is received. If the input/output controller 122 determines in step S222 that the playback command from the HDD 114 is a command for content that does not have to be protected, in step S223, the recording/playback processor 123 plays back the specified content from the optical disc 141.

[0187]

If the input/output controller 122 determines in step S224 that UC(0, S) of the user control data corresponding to

the content is "1", the content is found to be content that does not have to be protected on the bus 113. Then, in step S225, the content played back by the recording/playback processor 123 is directly (as the raw data) output to the HDD 114 via the bus 113.

[0188]

If it is determined in step S222 that the command from the HDD 114 is a playback command for content to be protected, or if it is determined in step S224 that UC(0, S) associated with the content is not "1", an error occurs since content to be protected on the bus 113 cannot be output to the unauthenticated HDD 114. Then, the recording processing by the drive 111 is forcefully terminated.

[0189]

As discussed above, when the protection information "1" is played back in response to the playback command from the HDD 114, the played back content that does not have to be protected on the bus 113 is directly output (without being encrypted) to the HDD 114 via the bus 113. Accordingly, since the content that does not have to be protected is not encrypted with a common key, it can be supplied to and stored in the HDD 14. Thus, the storage capacity of the HDD 14 can be efficiently utilized.

[0190]

Fig. 24 illustrates a still another example of the

configuration of the recording/playback apparatus to which the present invention is applied. The basic configuration of a recording/playback apparatus 401 shown in Fig. 24 is similar to the recording/playback apparatus 101 shown in Fig. 4. However, the content protector 132 of the AV board 112 shown in Fig. 4 is removed from the AV board 112 shown in Fig. 24, and instead, a content protector 411 is disposed in the drive 111.

[0191]

Accordingly, in the AV board 112 shown in Fig. 24, content supplied from the AV content processor 133 is output to the mutual authentication unit 131, and content output from the mutual authentication unit 131 is supplied to the AV content processor 133.

[0192]

In the drive 111 shown in Fig. 24, content input into the mutual authentication unit 121 is supplied to the content protector 411. The basic configuration of the content protector 411 is similar to that of the content protector 132 shown in Fig. 4. Accordingly, under the control of the input/output controller 122, the content protector 411 encrypts the content supplied from the mutual authentication unit 121 with the block key obtained from the disc ID and RKB (disc key) of the optical disc 141 or the block key obtained only from the RKB (disc key), and outputs

the encrypted content to the recording/playback processor 123.

[0193]

The recording/playback processor 123 supplies the content played back from the optical disc 141 to the content protector 411. The content protector 411 decrypts, under the control of the input/output controller 122, the content with the block key obtained from the disc ID and RKB of the optical disc 141 or the block key obtained only from the RKB, and outputs the decrypted content to the mutual authentication unit 121.

[0194]

Fig. 25 illustrates the configuration of the content protector 411 shown in Fig. 24. The configuration of the content protector 411 shown in Fig. 24 is basically similar to that of the content protector 132 shown in Fig. 9. Accordingly, if, for example, the input/output controller 122 determines that the content supplied from the AV board 112 is content to be protected (the recording command of the input content is a command for content to be protected), the encryption unit 254 encrypts the content with a block key for content to be protected, which is generated from the disc key, the disc ID, and recording information.

[0195]

If the input/output controller 122 determines that the

content input from the AV board 112 is content that does not have to be protected (the recording command of the input content is a command for content that does not have to be protected), the encryption unit 254 encrypts the content with a block key for content that does not have to be protected, which is generated from the disc key obtained from at least the RKB. The reason for using the disc key obtained from the RKB is to exclude unauthorized drives. The block key for content to be protected and the block key for content that does not have to be protected are generated by block-key generation processing, which is described below, with reference to Fig. 26, every time the optical disc 141 is installed in the drive 111, and the generated block keys are then stored in a built-in memory (not shown) of the encryption unit 254.

[0196]

A description is now given of the block-key generation processing performed by the content protector 411 shown in Fig. 24 with reference to the flowchart of Fig. 26.

[0197]

In step S241, the recording/playback processor 123 waits until the optical disc 141 is loaded into the drive 111. If it is determined in step S241 that the optical disc 141 is loaded, in step S242, the recording/playback processor 123 plays back the disc ID and RKB (disc

information) recorded on the optical disc 141 and supplies them to the content protector 411.

[0198]

In step S243, the RKB processor 252 obtains the disc key by using the supplied RKB, and the device ID and device key stored in the built-in memory. This processing is similar to that of step S123 of Fig. 16, and an explanation thereof is thus omitted to avoid repeated explanations.

[0199]

In step S244, the key generator 253 generates a block key for content to be protected by using the disc ID supplied from the recording/playback processor 123, the disc key generated in step S243, and the recording information of the content protector 411, and stores the generated block key in the built-in memory of the encryption unit 254.

[0200]

In step S245, the key generator 253 generates a block key for content that does not have to be protected by using at least the disc key generated in step S243, and stores the generated block key in the built-in memory of the encryption unit 254.

[0201]

As described above, in the content protector 411 shown in Fig. 24, every time the optical disc 141 is installed, two types of block keys for content to be protected and for

content that does not have to be protected are generated and stored. Although in the above description the block keys are generated, the disc ID and the disc key for generating block keys may be stored, and, when encrypting content, the block key may be generated according to the protection state of the content.

[0202]

A description is now given of recording request processing performed by the AV board 112 shown in Fig. 24 with reference to the flowchart of Fig. 27. The recording request processing shown in Fig. 27 is similar to that of Fig. 15, except that steps S103 and S104 of the recording request processing of Fig. 15 are removed.

[0203]

In the drive 111, mutual authentication has been conducted to share the common key with the AV board 112 when performing processing after the processing of Fig. 27.

[0204]

In step S261, the AV content processor 133 receives content. If the AV content processor 133 determines in step S262 that the content is to be protected, in step S263, the mutual authentication unit 131 encrypts the content with the common key shared with the drive 111. In step S264, the encrypted content is output to the drive 111. If it is determined in step S262 that the content does not have to be

protected, the content is not encrypted (step S263 is skipped), and is output to the drive 111 in step S264.

[0205]

As discussed above, content to be protected is encrypted with the common key shared with the drive 111 and is output from the AV board 112. Content that does not have to be protected is directly output from the AV board 112. Recording processing executed by the drive 111 shown in Fig. 24 in response to this processing is described below with reference to the flowchart of Fig. 28. Steps S301 through S304, steps S306 and S307, and steps S309 and S310 of Fig. 28 are similar to steps S161 through S168 of Fig. 18, and a detailed explanation thereof is thus omitted.

[0206]

In step S301, the mutual authentication unit 121 of the drive 111 receives the content from the AV board 112 via the bus 113.

[0207]

In step S302, the input/output controller 122 determines whether the AV board 112 that has sent the content has been mutually authenticated in the drive 111 based on the information from the mutual authentication unit 121. If it is determined that the AV board 112 has been mutually authenticated in the drive 111, in step S303, the input/output controller 122 determines whether the recording

command of the input content is for content to be protected on the bus 113 based on whether the content input into the mutual authentication unit 121 is encrypted with the common key.

[0208]

If it is determined in step S303 that the recording command of the input content is for content to be protected on the bus 113, in step S304, the input/output controller 122 controls the mutual authentication unit 121 to decrypt the received content with the common key shared with the AV board 112 and to supply the content to the content protector 411.

[0209]

In step S305, the encryption unit 254 encrypts the supplied content by using the block key for content to be protected. This block key for content to be protected has been stored in the memory of the encryption unit 254, as described with reference to Fig. 26. Then, in step S306, the input/output controller 122 controls the recording/playback processor 123 to generate and store protection information "0", which indicates that this content should be protected on the bus 113, in UC(0, S) of the user control data associated with this content. In step S310, the input/output controller 122 controls the recording/playback processor 123 to record the protection

information on the optical disc 141 together with the content encrypted with the block key for content to be protected.

[0210]

On the other hand, for example, content stored in the HDD 114 without a mutual authentication unit is input. In this case, in step S301, content from the HDD 114 is received by the mutual authentication unit 121 via the bus 113. In step S302, it is determined that the device which has sent this content has not been mutually authenticated in the drive 111. In step S307, the input/output controller 122 determines whether the recording command of the input content is a command for content to be protected on the bus 113 based on whether the content input into the mutual authentication unit 121 is encrypted with the common key.

[0211]

If it is determined in step S303 or S307 that the recording command of the input content is for content that does not have to be protected on the bus 113, the process proceeds to step S308. In step S308, the encryption unit 254 encrypts the content supplied from the mutual authentication unit 121 by using the block key for content that does not have to be protected. This block key for content that does not have to be protected has been stored in the memory of the encryption unit 254, as discussed with

reference to Fig. 26.

[0212]

In step S309, the input/output controller 122 controls the recording/playback processor 123 to generate and store protection information "1", which indicates that this content does not have to be protected on the bus 113, in UC(0, S) of the user control data corresponding to this content. In step S310, the input/output controller 122 controls the recording/playback processor 123 to record the generated protection information on the optical disc 141 together with the content.

[0213]

If it is determined in step S307 that the recording command of the input content is for content to be protected on the bus 113, an error occurs, and the recording processing by the drive 111 is forcefully terminated.

[0214]

As discussed above, content to be protected supplied from the authenticated AV board 112 is encrypted with the block key obtained from the disc ID and RKB, and is recorded on the optical disc 141 together with the protection information "0", which means that this content should be protected on the bus 113. In contrast, content that does not have to be protected supplied from the authenticated AV board 112, or content that does not have to be protected

from the unauthenticated HDD 114 is encrypted with the block key obtained only from the RKB, and is recorded on the optical disc 141 together with the protection information "1", which indicates that this content does not have to be protected on the bus 113. Content that should be protected from the unauthenticated HDD 114 is not recorded on the optical disc 141.

[0215]

Content playback processing by the drive 111 shown in Fig. 24 is described below with reference to the flowchart of Fig. 29. Steps S321 through S325 and steps S327 through S330 of Fig. 29 are similar to steps S191 through S200 of Fig. 19, and a detailed explanation thereof is thus omitted.

[0216]

In order to output content to be protected recorded on the optical disc 141 from the output unit 135 of the AV board 112, the user inputs a content playback command into the AV board 112 via the operation input unit. The mutual authentication unit 131 of the AV board 112 sends the playback command to the drive 111 via the bus 113. In step S321, the mutual authentication unit 121 receives the playback command from the AV board 112. If it is determined in step S322 based on the information from the mutual authentication unit 121 that the AV board 112 which receives the content has been mutually authenticated in the drive 111,

the input/output controller 122 determines in step S323 whether the playback command from the AV board 112 is for content to be protected.

[0217]

If it is determined in step S323 that the playback command from the AV board 112 is for content to be protected, in step S324, the recording/playback processor 123 plays back the specified content from the optical disc 141. If the input/output controller 122 determines in step S325 that UC(0, S) of the user control data corresponding to the content is "0", the played back content is found to be content to be protected on the bus 113. In step S326, the encryption unit 254 decrypts the played back content by using the block key for content to be protected stored in the built-in memory. In step S327, the mutual authentication unit 121 encrypts the content supplied from the encryption unit 254 by using the common key shared with the AV board 112, and outputs the content to the AV board 112 via the bus 113.

[0218]

In contrast, in order to store (record) in the HDD 114 content recorded on the optical disc 141 that does not have to be protected, the user inputs a content playback command into the HDD 114 by operating the operation input unit. The HDD 114 sends the playback command to the drive 111 via the

bus 113. Then, in step S321, the mutual authentication unit 121 receives the playback command from the HDD 114. It is then determined in step S322 that the HDD 114 which receives the content is not mutually authenticated based on the information from the mutual authentication unit 121. Then, it is determined in step S328 whether the playback command from the HDD 114 is a command for content to be protected.

[0219]

If it is determined in step S323 or S228 that the playback command from the HDD 114 is a command for content that does not have to be protected, in step S329, the recording/playback processor 123 plays back the specified content from the optical disc 141. Then, in step S330, the input/output controller 122 determines whether UC(0, S) of the user control data associated with this content is "1". If the input/output controller 122 determines in step S230 that UC(0, S) of the user control data associated with this content is "1", the played back content is found to be content that does not have to be protected on the bus 113. In step S331, the encryption unit 254 decrypts the content with the block key for content that does not have to be protected stored in the built-in memory, and directly outputs the content (as the raw data) to the AV board 112 or the HDD 114 via the mutual authentication unit 121 and the bus 113.

[0220]

If it is determined in step S325 that UC(0, S) corresponding to the content is not "0", or if it is determined in step S328 that the playback command from the HDD 114 is a command for content to be protected, or if it is determined in step S330 that UC(0, S) corresponding to the content is not "1", an error occurs, and the recording processing by the drive 111 is forcefully terminated.

[0221]

As discussed above, in response to the playback command from the authenticated AV board 112, content to be protected on the bus 113 is encrypted with the common key and is output to the AV board 112 via the bus 113. Content that does not have to be protected on the bus 113 is directly output (without being encrypted) to the AV board 112 via the bus 113. Then, in step S361 of Fig. 30, which is described below, the content is received by the mutual authentication unit 131 of the AV board 112.

[0222]

Playback processing by the AV board 112 corresponding to the content playback processing by the drive 111 shown in Fig. 24 is described below with reference to the flowchart of Fig. 30. The playback processing shown in Fig. 30 is similar to that shown in Fig. 20, except that steps S204 and S205 of the playback processing shown in Fig. 20 are removed.

[0223]

In step S361, the mutual authentication unit 131 receives the content from the drive 111. If it is determined in step S362 that the content is encrypted with the common key, i.e., the content is to be protected, in step S363, the content is decrypted with the common key shared with the drive 111.

[0224]

If it is determined in step S362 that the content is not encrypted, i.e., the content does not have to be protected, it is not necessary to decrypt this content because the content has not been encrypted. Accordingly, the content passes through the mutual authentication unit 131 and the content protector 132, and thus, step S363 is skipped.

[0225]

In step S364, the AV content processor 133 decodes the content supplied from the content protector 132 according to, for example, an MPEG method, and plays back the content. In step S365, the output unit 135 outputs the played back content.

[0226]

As described above, from the AV board 112, which is authenticated with the drive 111, content recorded on the optical disc 141 which is to be protected on the bus 113 and

content that does not have to be protected on the bus 113 can be output.

[0227]

Fig. 31 illustrates another example of the configuration of the recording/playback apparatus of the present invention. The basic configuration of a recording/playback apparatus 501 shown in Fig. 31 is similar to that of the recording/playback apparatus 401 shown in Fig. 24, except that the mutual authentication unit 121 of the drive 111 in the recording/playback apparatus 401 shown in Fig. 24 is removed from the recording/playback apparatus 501 in Fig. 31.

[0228]

Accordingly, in the recording/playback apparatus 501 shown in Fig. 31, even though the AV board 112 is connected to the bus 113, the drive 11 is not mutually authenticated in the AV board 112 since the drive 111 is not provided with a mutual authentication function (a common key is not shared). Thus, although content-playback-request processing in response to a request from the AV board 112 is not executed in the drive 111, the drive 111 can send and receive content that does not have to be protected to and from the HDD 114 which is not provided with a mutual authentication function.

[0229]

The recording processing performed by the drive 111 of the recording/playback apparatus 501 is described below with reference to the flowchart of Fig. 32. Steps S401 through S405 of Fig. 32 are similar to step S301 and steps S307 through S310 of Fig. 28, and an explanation thereof is thus omitted.

[0230]

In step S401, the recording/playback processor 123 receives content that does not have to be protected from the HDD 114 via the bus 113. In step S402, the input/output controller 122 determines that the recording command of the input content is not a command for content to be protected on the bus 113 based on whether the content input into the mutual authentication unit 121 is encrypted with the common key. In step S403, the encryption unit 254 encrypts the content by using the block key for content that does not have to be protected.

[0231]

In step S404, the recording/playback processor 123 generates and stores protection information "1", which indicates that this content does not have to be protected on the bus 113, in UC(0, S) of the user control data corresponding to the content. In step S405, the recording/playback processor 123 records the protection information "1" on the optical disc 141 together with the

content supplied from the HDD 114 that does not have to be protected.

[0232]

If content encrypted with the common key is input, and if it is determined in step S402 that the recording command of the input content is a command for content to be protected on the bus 113, an error occurs, and the recording processing by the drive 111 is forcefully terminated. If the content is not encrypted with the common key, but is encrypted by another method, it may be determined that the content does not have to be protected on the bus 113.

[0233]

As discussed above, content that does not have to be protected on the bus 113 supplied from the HDD 114 without a mutual authentication function is recorded on the optical disc 141.

[0234]

A description is now given of playback processing performed by the drive 111 in the recording/playback apparatus 501 with reference to the flowchart of Fig. 33. Steps S421 through S425 of Fig. 33 are similar to step S321 and steps S328 through S331 of Fig. 29, and a detailed explanation thereof is thus omitted.

[0235]

For example, in order to store (record) in the HDD 114

content recorded on the optical disc 141 that does not have to be protected, the user inputs a content playback command into the HDD 114 via the operation input unit. The HDD 114 sends the playback command to the drive 111 via the bus 113. In step S421, the playback command from the HDD 114 is input, and if it is determined in step S422 that the playback command from the HDD 114 is for content that does not have to be protected, the process proceeds to step S423. In step S423, the recording/playback processor 123 plays back the specified content from the optical disc 141.

[0236]

If the input/output controller 122 determines in step S424 that UC(0, S) of the user control data corresponding to the content is "1", it means that the played back content is found to be content that does not have to be protected on the bus 113. In step S425, the encryption unit 254 decrypts the content by using the block key for content that does not have to be protected, and directly outputs the content (as the raw data) to the AV board 112 or the HDD 114 via the mutual authentication unit 121 and the bus 113.

[0237]

In contrast, if it is determined in step S422 that the command from the HDD 114 is a playback command for content to be protected, or if it is determined in step S424 that UC(0, S) corresponding to the content is not "1", an error

occurs since content to be protected cannot be output to the unauthenticated HDD 114. Then, the recording processing by the drive 111 is forcefully terminated.

[0238]

In this manner, in response to the playback command from the HDD 114, the protection information "1" is played back, and the played back content that does not have to be protected is directly output (without being encrypted) to the HDD 114 via the bus 113. Accordingly, content that does not have to be protected on the bus 113 is not encrypted, and thus, it can be supplied to the HDD 114 and stored.

[0239]

Even if content from the unauthenticated HDD 114 is indicated as content to be protected, it is not recognized as content to be protected in the drive 111. Only content that does not have to be protected can be processed in the drive 111. Accordingly, unauthenticated storage devices that handle only copy free content can be efficiently utilized.

[0240]

Although in the above description the recording medium is the optical disc 141, it may be another type of recording medium, for example, a memory card (registered trademark), in addition to the optical disc 141.

[0241]

A series of the above-described processing may be executed by hardware or software. In this case, the recording/playback apparatus 101 shown in Fig. 4, the recording/playback apparatus 301 shown in fig. 21, the recording/playback apparatus 401 shown in Fig. 24, or the recording/playback apparatus 501 shown in Fig. 31, can be formed by, for example, a recording/playback apparatus 601 shown in Fig. 34.

[0242]

In Fig. 31, a CPU (Central Processing Unit) 611 executes various types of processing according to programs stored in a ROM (Read Only Memory) 612 or programs loaded into a RAM (Random Access Memory) 613 from an HDD 619. In the RAM 613, data necessary for the CPU 611 to perform various types of processing is suitably stored.

[0243]

The CPU 611, the ROM 612, and the RAM 613 are connected to each other via a bus 614. An input/output interface 615 is also connected to the bus 614.

[0244]

The input/output interface 615 is connected to an AV board 616 for controlling the input/output of content, an input unit 617 including, for example, a keyboard and a mouse, an output unit 618 including, for example, a display device such as a CRT (Cathode Ray Tube) or LCD (Liquid

Crystal Display), and a speaker, the HDD 619, and a communication unit 620 including, for example, a modem or a terminal adapter. The communication unit 620 performs communication processing via the bus or a network (not shown).

[0245]

A drive 630 is connected to the input/output interface 615 when necessary. A magnetic disk 631, an optical disc 632, a magneto-optical disk 633, or a semiconductor memory 634 is suitably loaded into the drive 630, and a computer program read from such a recording medium is installed into the HDD 619 if necessary.

[0246]

If the above-described series of processing is executed by software, a corresponding software program is installed via a network or a recording medium into a computer built into dedicated hardware or into a computer that can execute various functions by installing various programs therein, for example, a general-purpose personal computer.

[0247]

This recording medium includes a package medium, recording the program therein, consisting of the magnetic disk 631 (including flexible disks), the optical disc 632 (including CD-ROM (Compact Disk - Read Only Memory) and DVD (Digital Versatile Disk)), the magneto-optical disk 633

(including MD (Mini-Disk) (trademark)), or the semiconductor memory 634, as shown in Fig. 34, which is distributed for providing the program to the user separately from the apparatus. The recording medium also includes the ROM 612 or the HDD 619 recording the program therein, which is provided to the user while being integrated into the apparatus.

[0248]

Steps forming the program to be recorded on the recording medium may be executed in chronological order described in this specification. However, they may be executed concurrently or individually.

[0249]

In this specification, the system represents the entirety of an apparatus formed of a plurality of devices.

[0250]

[Advantages]

As is seen from the foregoing description, according to the present invention, content can be flexibly protected according to whether or not the content should be protected. Additionally, according to the present invention, unauthorized copying of content can be prevented. Data can also be stored in storage devices of a PC.

[Brief Description of the Drawings]

[Fig. 1]

Fig. 1 is a block diagram illustrating an example of the configuration of a known recording/playback apparatus.

[Fig. 2]

Fig. 2 is a block diagram illustrating another example of the configuration of a known recording/playback apparatus.

[Fig. 3]

Fig. 3 is a block diagram illustrating still another example of the configuration of a known recording/playback apparatus.

[Fig. 4]

Fig. 4 is a block diagram illustrating an example of the configuration of a recording/playback apparatus to which the present invention is applied.

[Fig. 5]

Fig. 5 illustrates an example of the configuration of the data format used in the present invention.

[Fig. 6]

Fig. 6 illustrates an example of the configuration of the data frame shown in Fig. 5.

[Fig. 7]

Fig. 7 illustrates an example of the configuration of the scramble data frame shown in Fig. 5.

[Fig. 8]

Fig. 8 illustrates an example of the configuration of the user control data shown in Fig. 5.

[Fig. 9]

Fig. 9 is a block diagram illustrating an example of the configuration of a content protector 132 shown in Fig. 4.

[Fig. 10]

Fig. 10 is a tree structure illustrating the disc key used in the present invention.

[Fig. 11]

Fig. 11 illustrates examples of RKBs used for the disc key of the present invention.

[Fig. 12]

Fig. 12 illustrates an example of applications of the RKBs shown in Fig. 11.

[Fig. 13]

Fig. 13 is a flowchart illustrating mutual authentication processing by an AV board shown in Fig. 4.

[Fig. 14]

Fig. 14 is a flowchart illustrating mutual authentication processing by a drive shown in Fig. 4.

[Fig. 15]

Fig. 15 is a flowchart illustrating recording request processing by the AV board shown in Fig. 4.

[Fig. 16]

Fig. 16 is a flowchart illustrating block-key generation processing in step S103 of Fig. 15.

[Fig. 17]

Fig. 17 is a flowchart illustrating disc-information playback processing by the drive shown in Fig. 4 corresponding to the processing of Fig. 16.

[Fig. 18]

Fig. 18 is a flowchart illustrating recording processing by the drive shown in Fig. 4.

[Fig. 19]

Fig. 19 is a flowchart illustrating playback processing by the drive shown in Fig. 4.

[Fig. 20]

Fig. 20 is a flowchart illustrating playback processing by the AV board shown in Fig. 4.

[Fig. 21]

Fig. 21 is a block diagram illustrating another example of the configuration of the recording/playback apparatus shown in Fig. 4.

[Fig. 22]

Fig. 22 is a flowchart illustrating recording processing by the drive shown in Fig. 21.

[Fig. 23]

Fig. 23 is a flowchart illustrating playback processing by the drive shown in Fig. 21.

[Fig. 24]

Fig. 24 is a block diagram illustrating still another example of the configuration of the recording/playback

apparatus of the present invention.

[Fig. 25]

Fig. 25 is a block diagram illustrating an example of the configuration of a content protector 411 shown in Fig. 24.

[Fig. 26]

Fig. 26 is a flowchart illustrating block-key generation processing by the drive shown in Fig. 24.

[Fig. 27]

Fig. 27 is a flowchart illustrating recording request processing by the AV board shown in Fig. 24.

[Fig. 28]

Fig. 28 is a flowchart illustrating recording processing by the drive shown in Fig. 24.

[Fig. 29]

Fig. 29 is a flowchart illustrating playback processing by the drive shown in Fig. 24.

[Fig. 30]

Fig. 30 is a flowchart illustrating playback processing by the AV board shown in Fig. 24.

[Fig. 31]

Fig. 31 is a block diagram illustrating another example of the configuration of the recording/playback apparatus shown in Fig. 24.

[Fig. 32]

Fig. 32 is a flowchart illustrating recording processing by the drive shown in Fig. 31.

[Fig. 33]

Fig. 33 is a flowchart illustrating playback processing by the drive shown in Fig. 31.

[Fig. 34]

Fig. 34 is a block diagram illustrating a further example of the configuration of the recording/playback apparatus of the present invention.

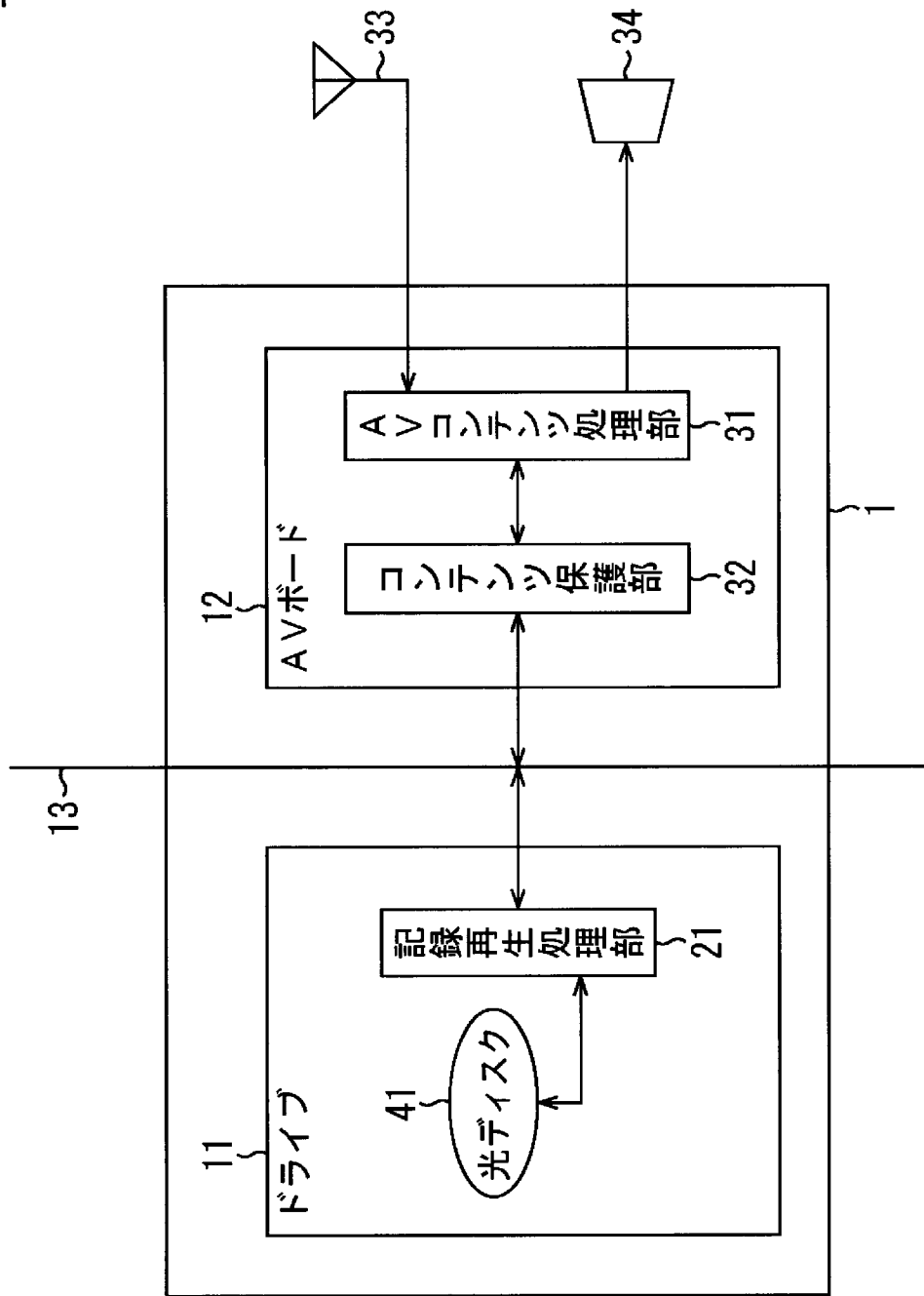
[Reference Numerals]

101: recording/playback apparatus, 111: drive, 112: AV board, 113: bus, 114: HDD, 121: mutual authentication unit, 122: input/output controller, 123: recording/playback processor, 131: mutual authentication unit, 132: content processor, 141: optical disc, 202: user control data, 252: RKB processor, 253: key generator, 254: encryption unit, 301: recording/playback apparatus, 401: recording/playback apparatus, 411: content protector, 501: recording/playback apparatus

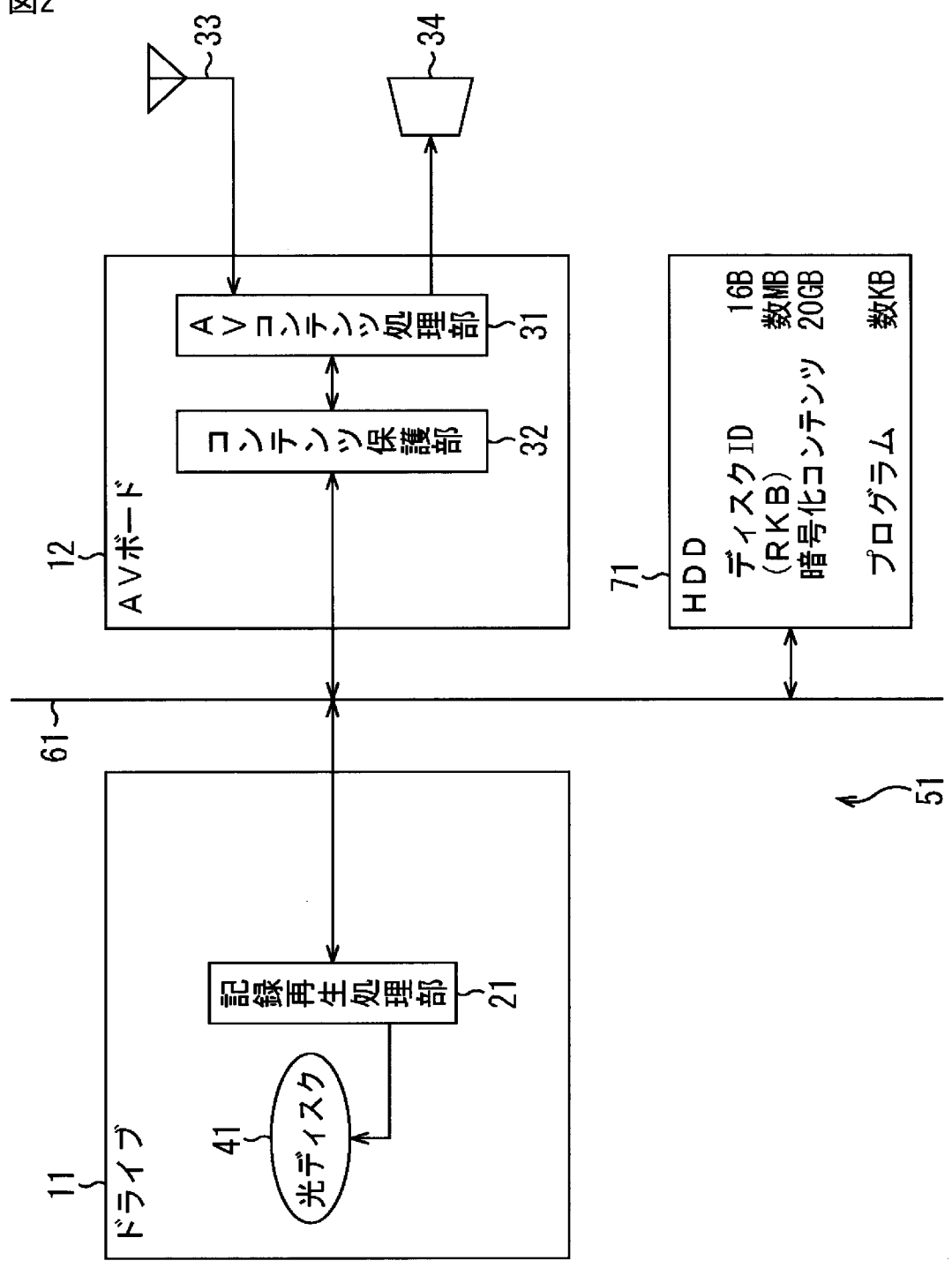
【書類名】 図面

【図 1】

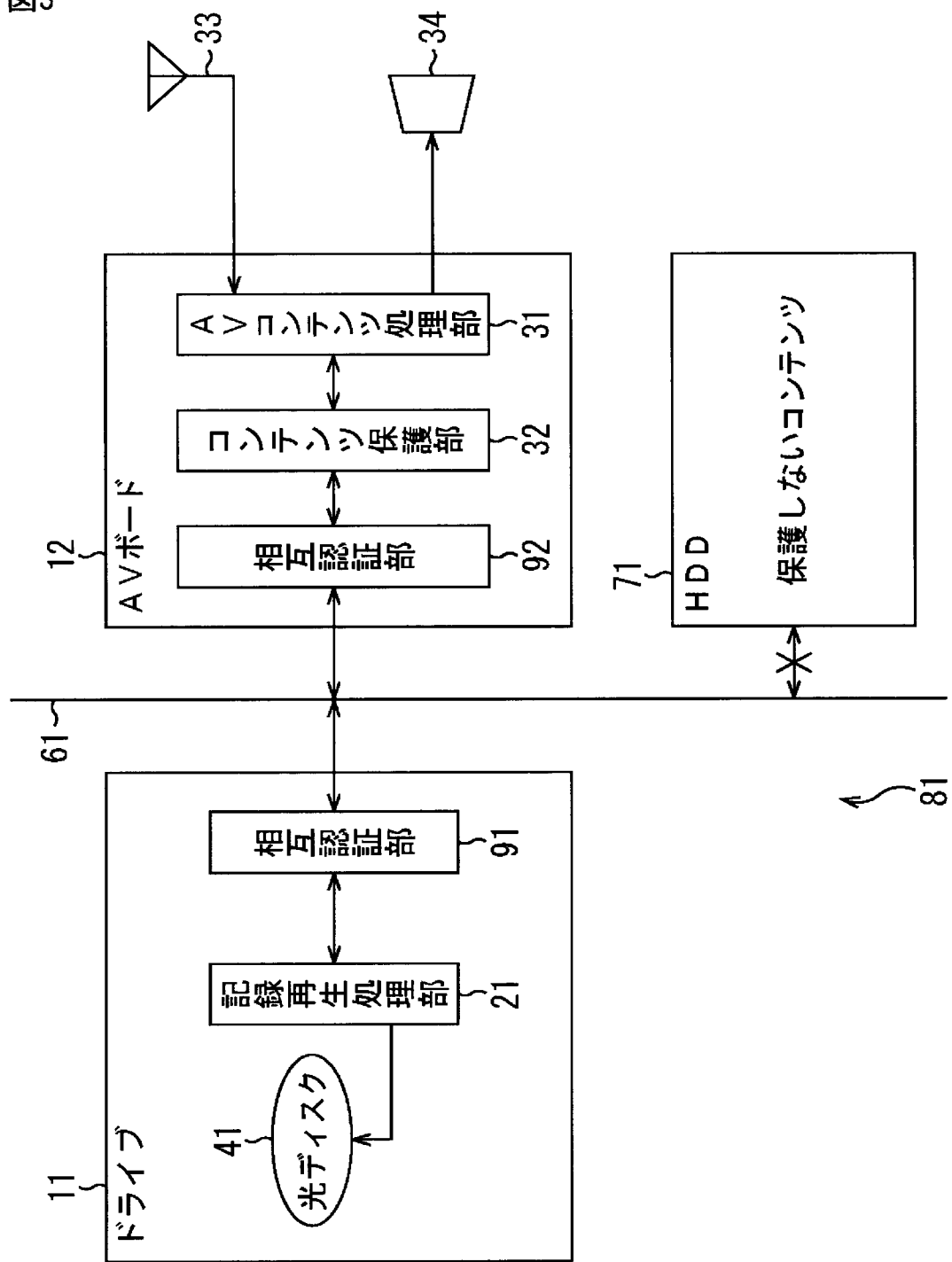
図1



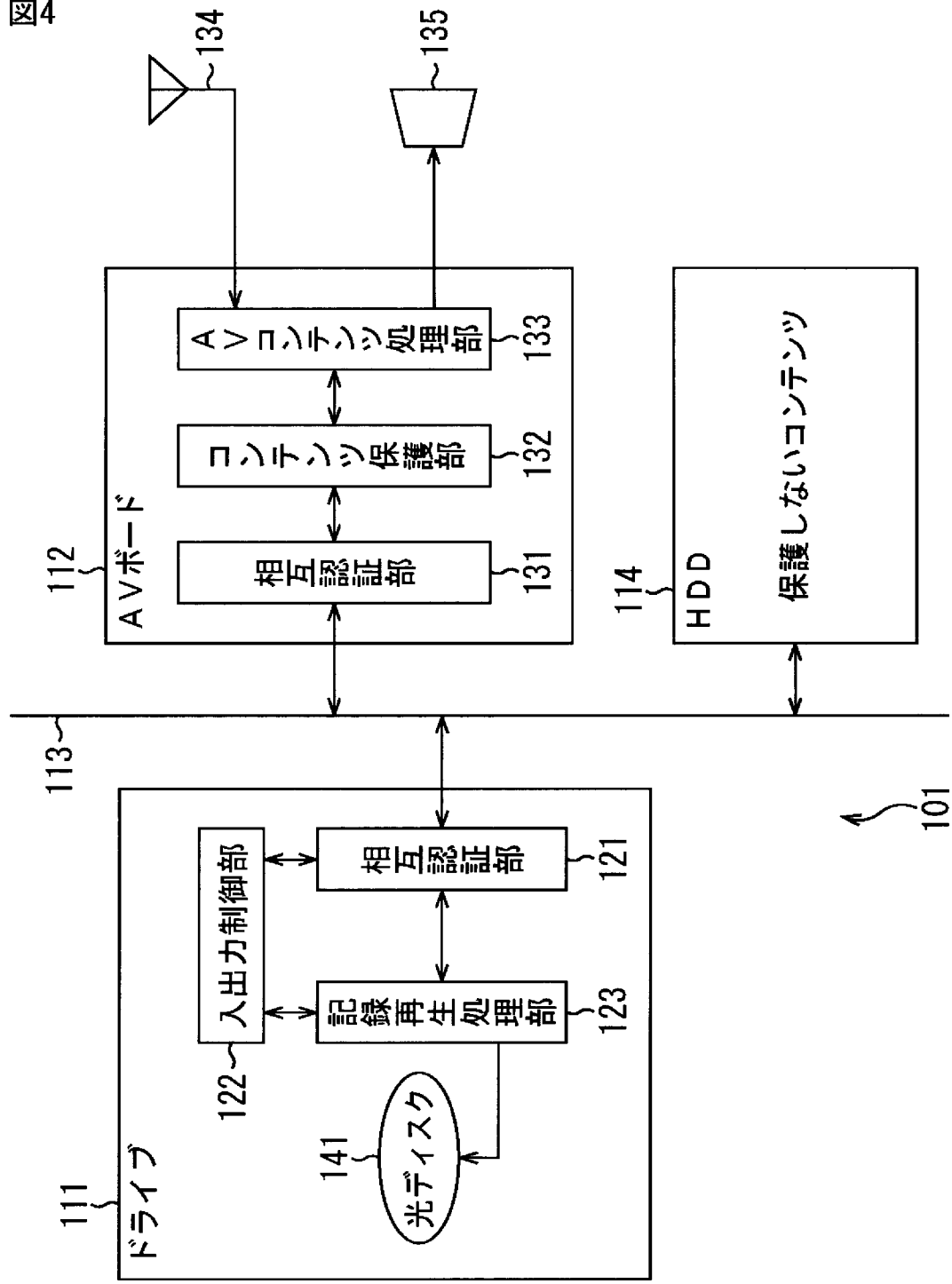
【図2】
図2



【図3】
図3

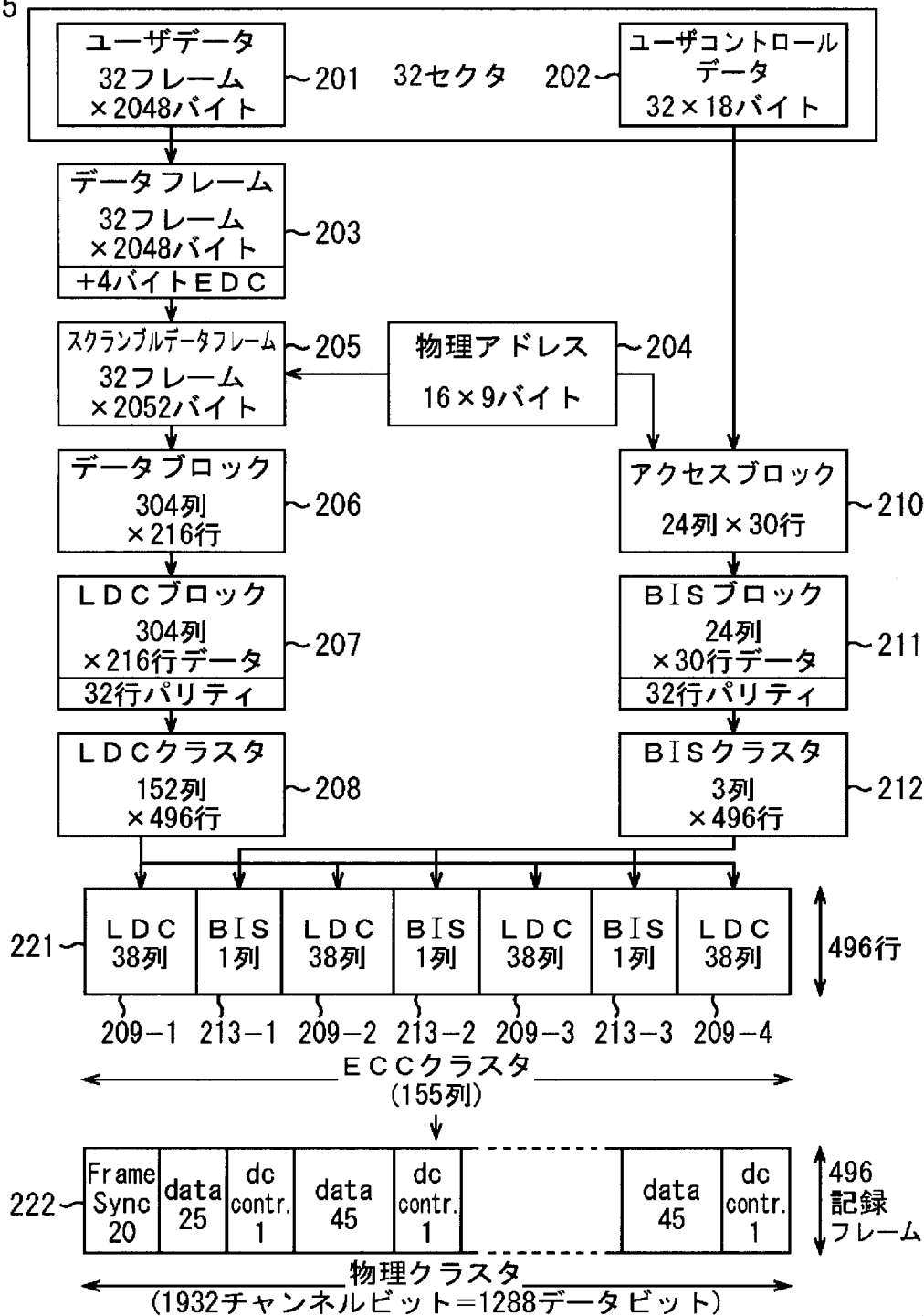


【図4】
図4



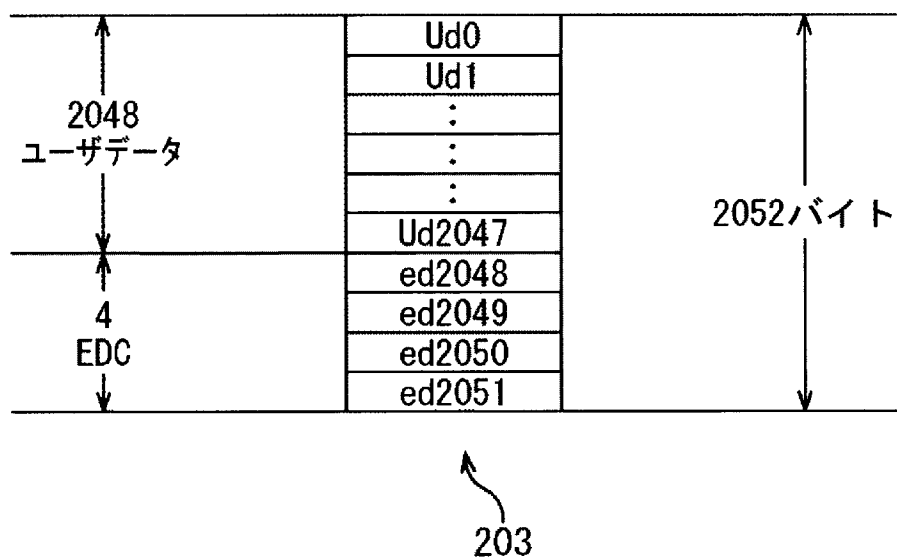
【図5】

図5



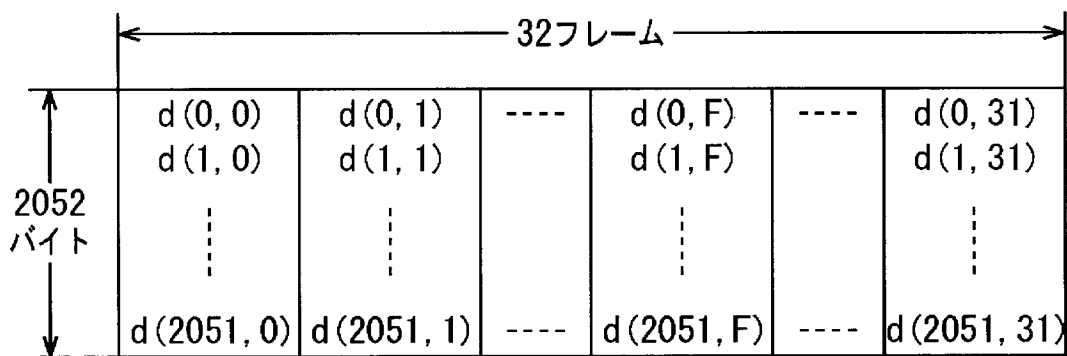
【図6】

図6



【図7】

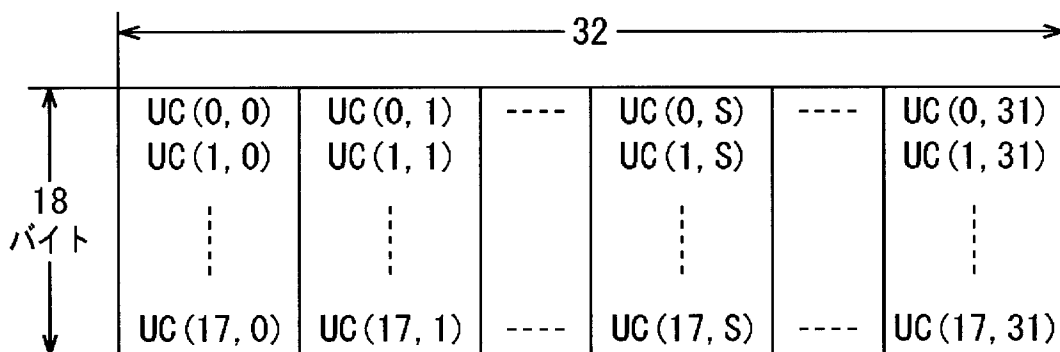
図7



205

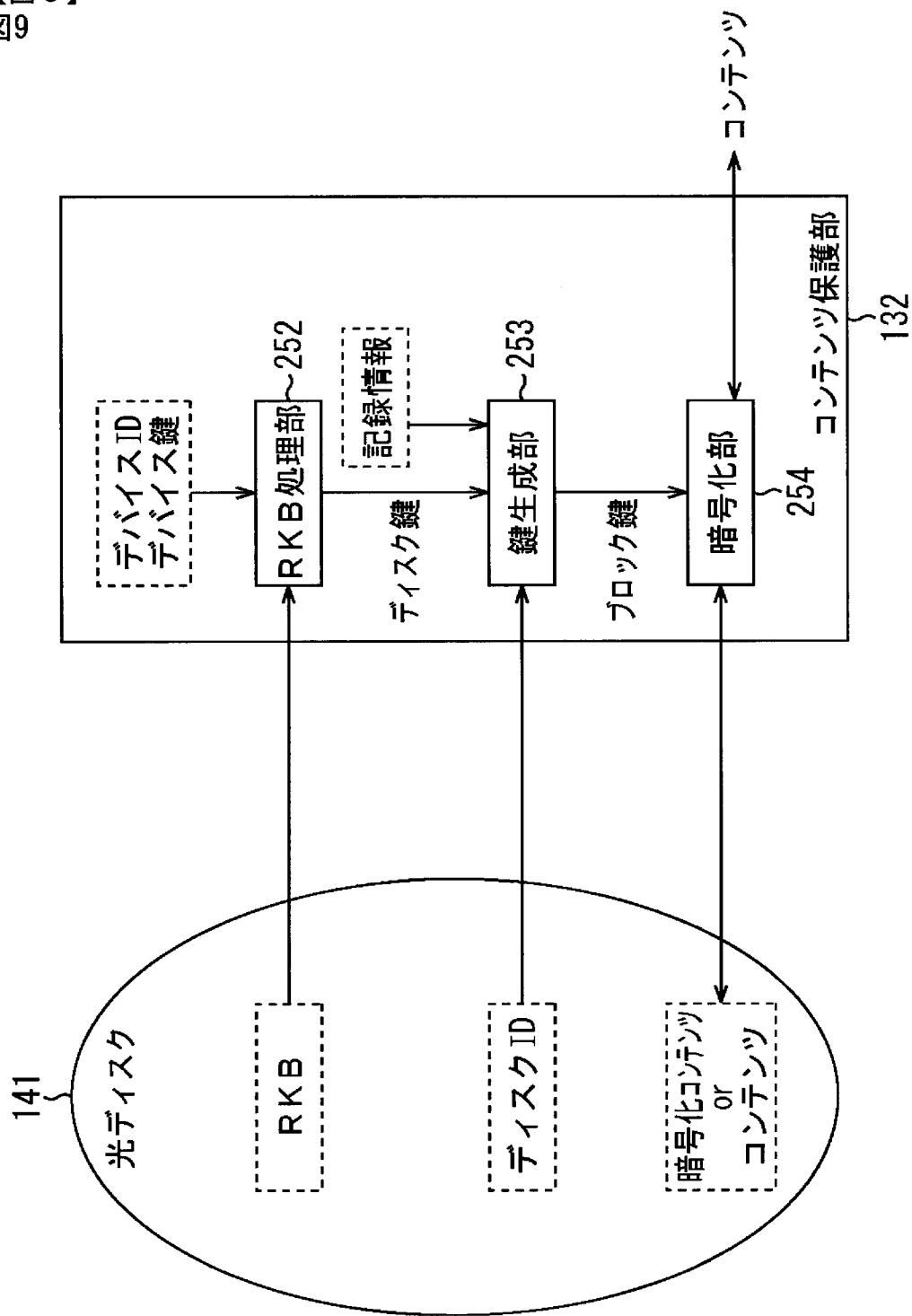
【図8】

図8

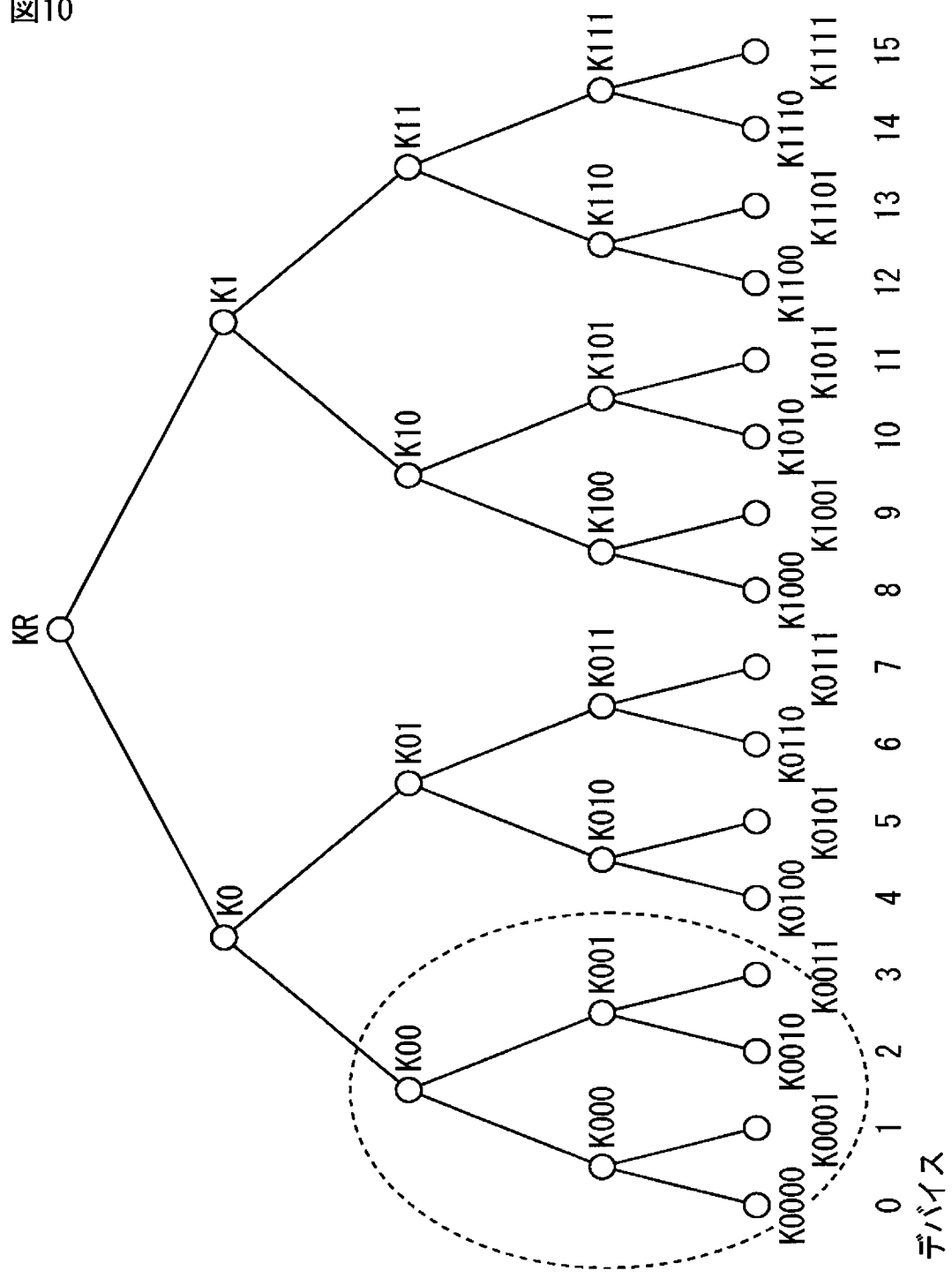


202

【図9】
図9



【図 10】
図10



【図 11】

図11

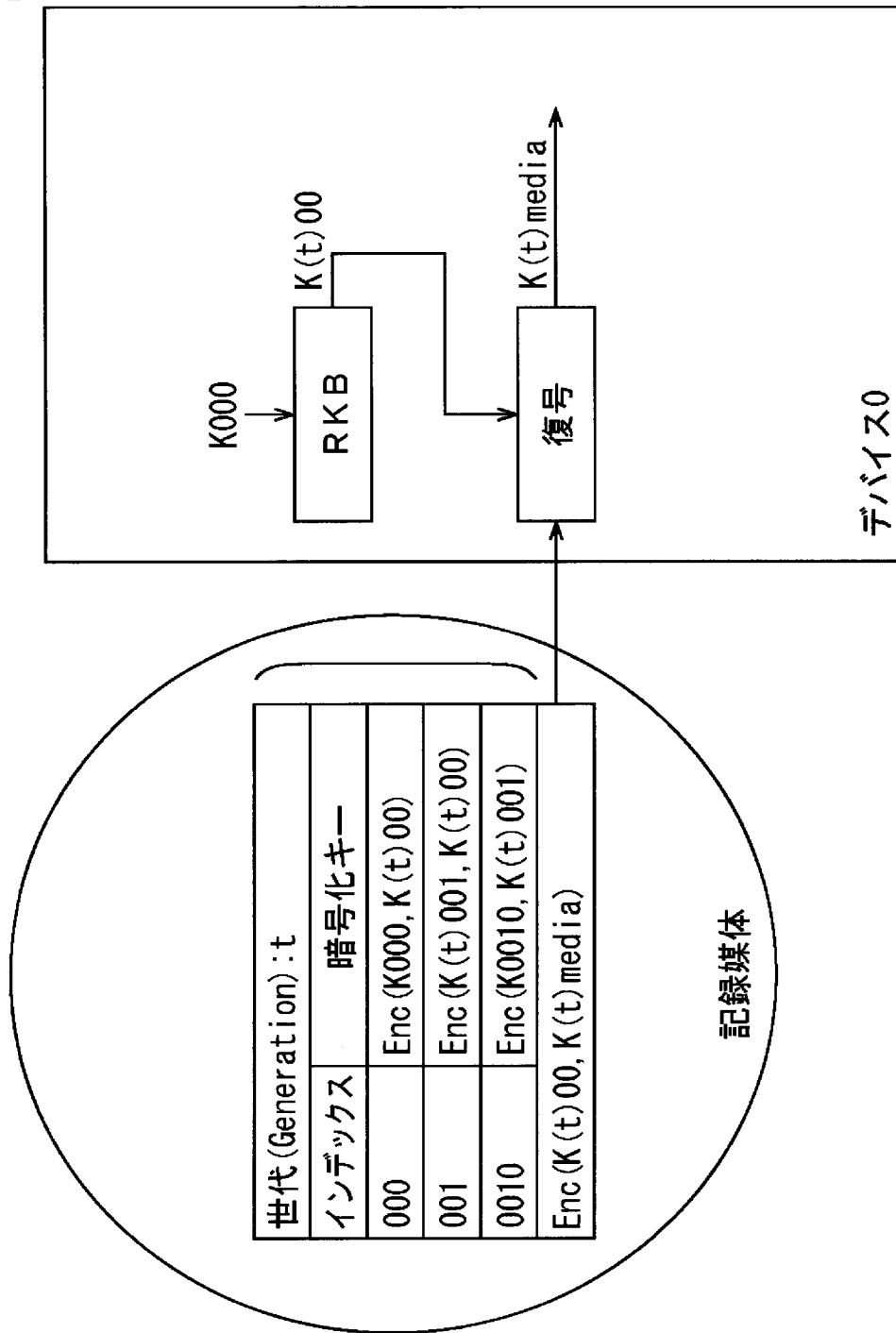
A

バージョン (Version) : t	
インデックス	暗号化キー
0	Enc (K (t) 0, K (t) R)
00	Enc (K (t) 00, K (t) 0)
000	Enc (K000, K (t) 00)
001	Enc (K (t) 001, K (t) 00)
0010	Enc (K0010, K (t) 001)

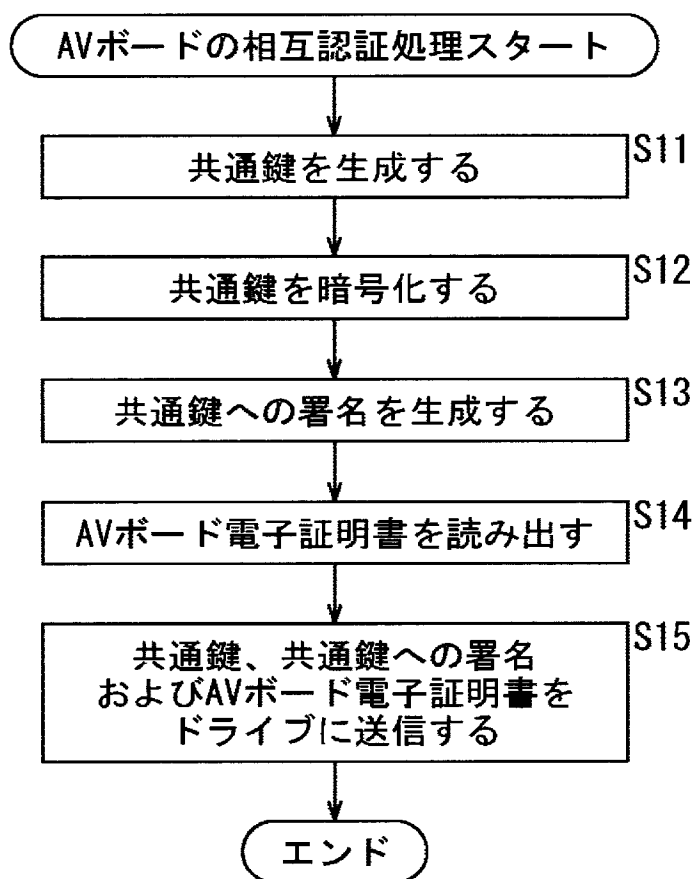
B

バージョン (Version) : t	
インデックス	暗号化キー
000	Enc (K000, K (t) 00)
001	Enc (K (t) 001, K (t) 00)
0010	Enc (K0010, K (t) 001)

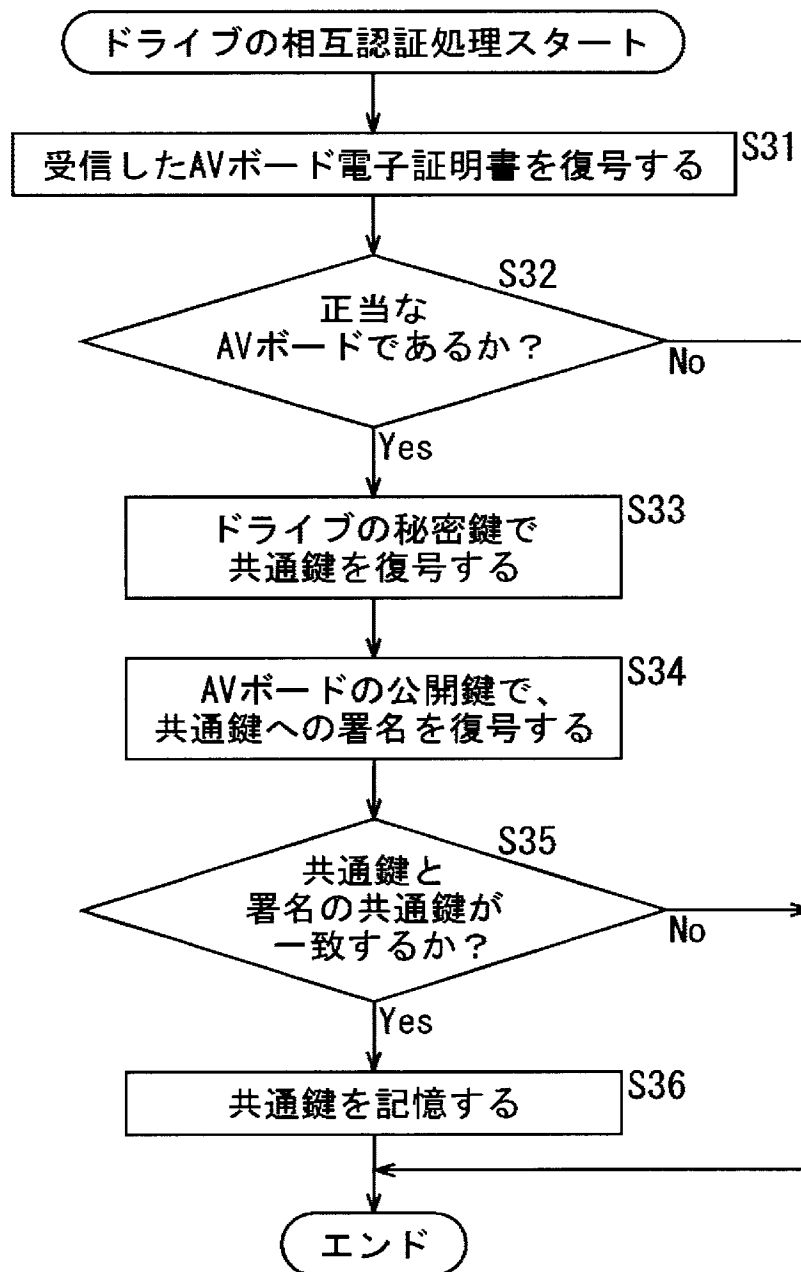
【図 12】
図12



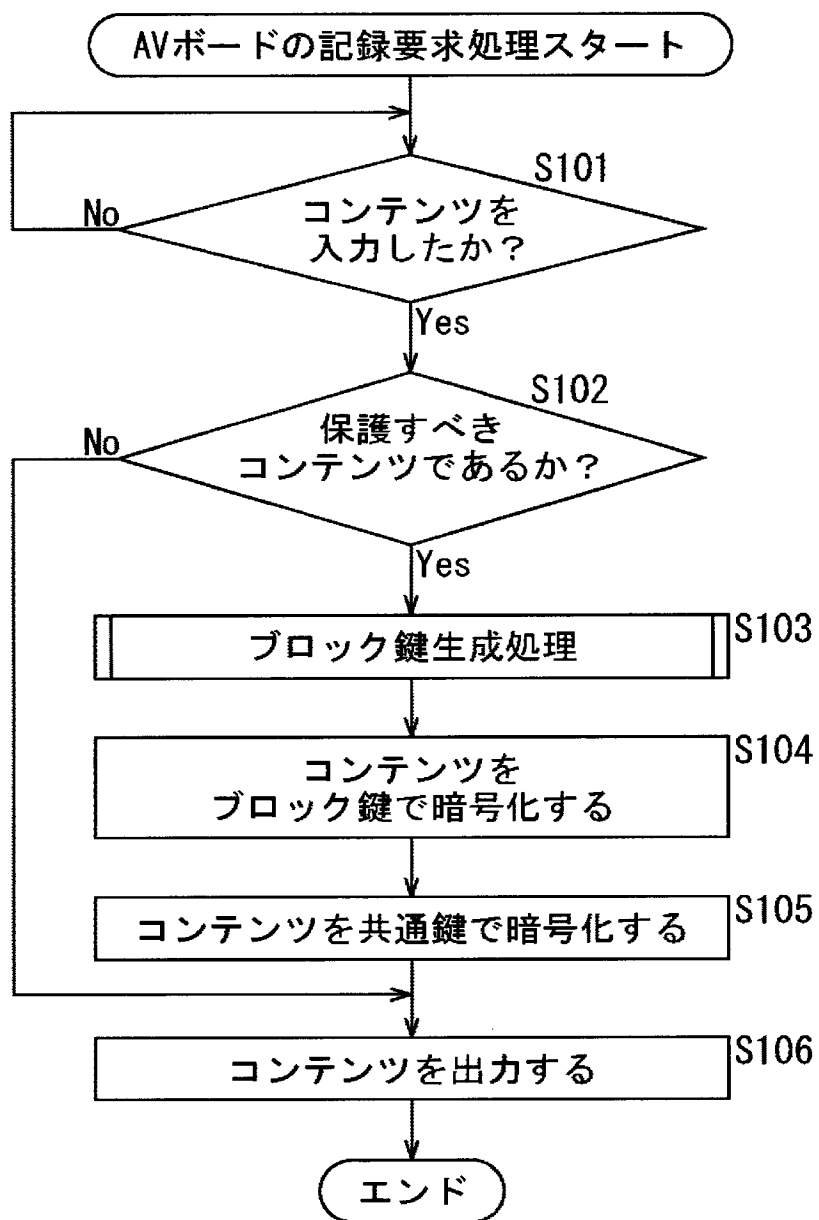
【図13】
図13



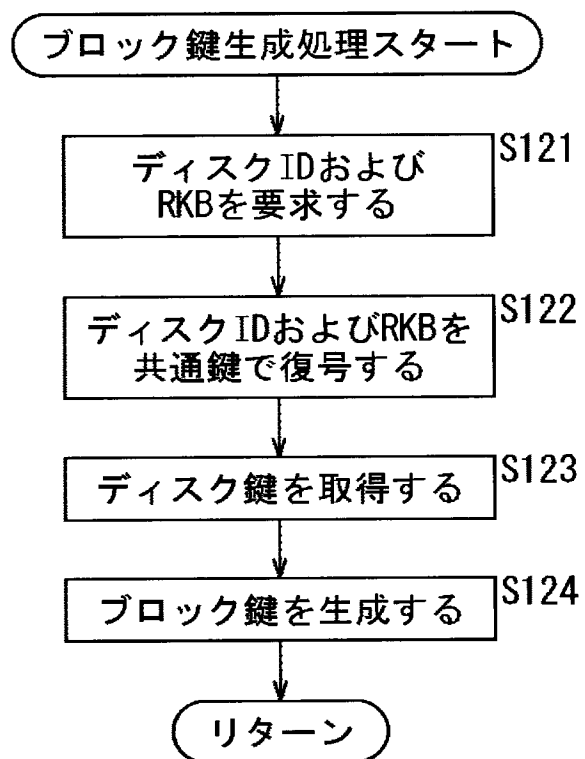
【図14】
図14



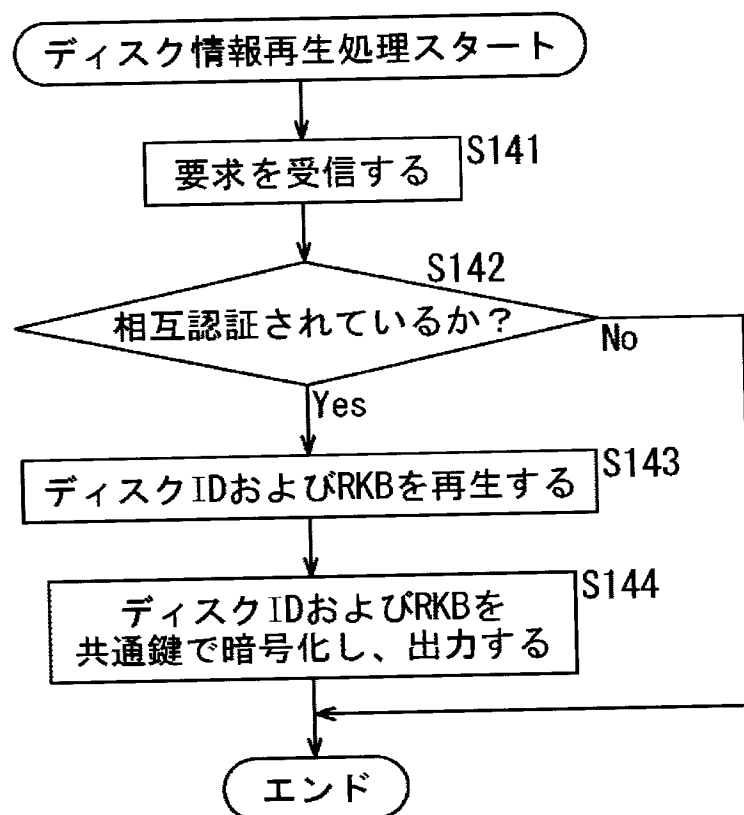
【図15】
図15



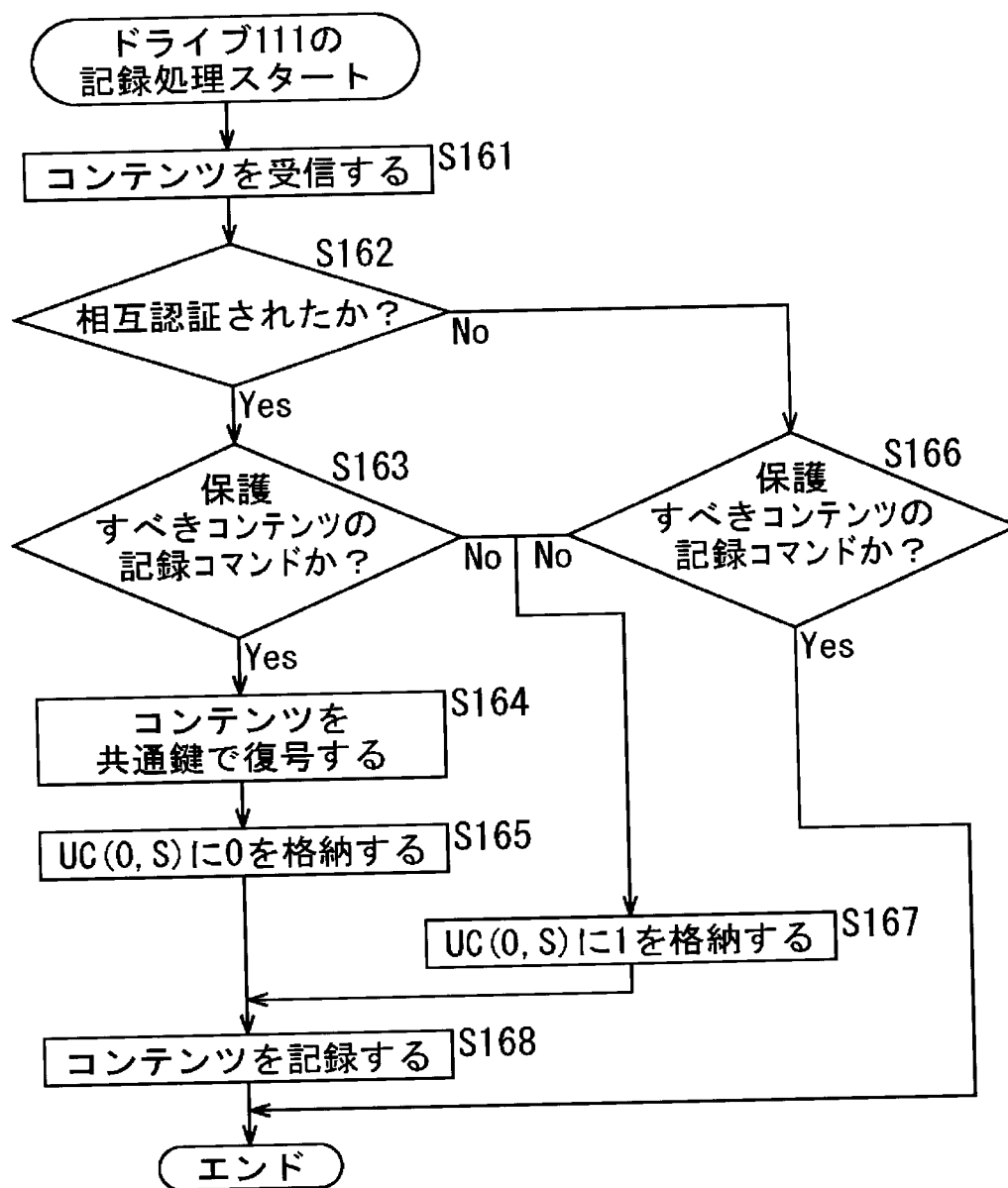
【図16】
図16



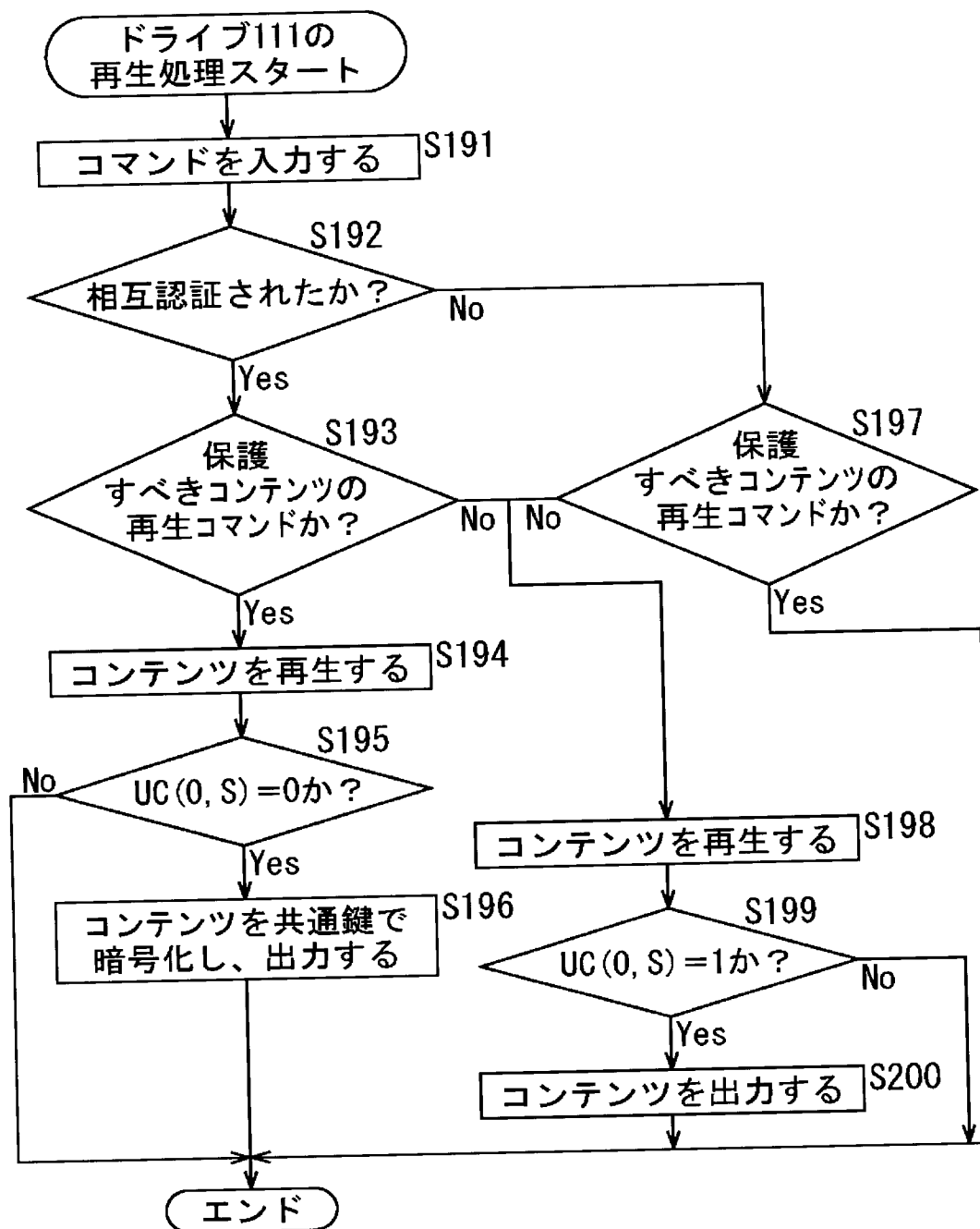
【図17】
図17



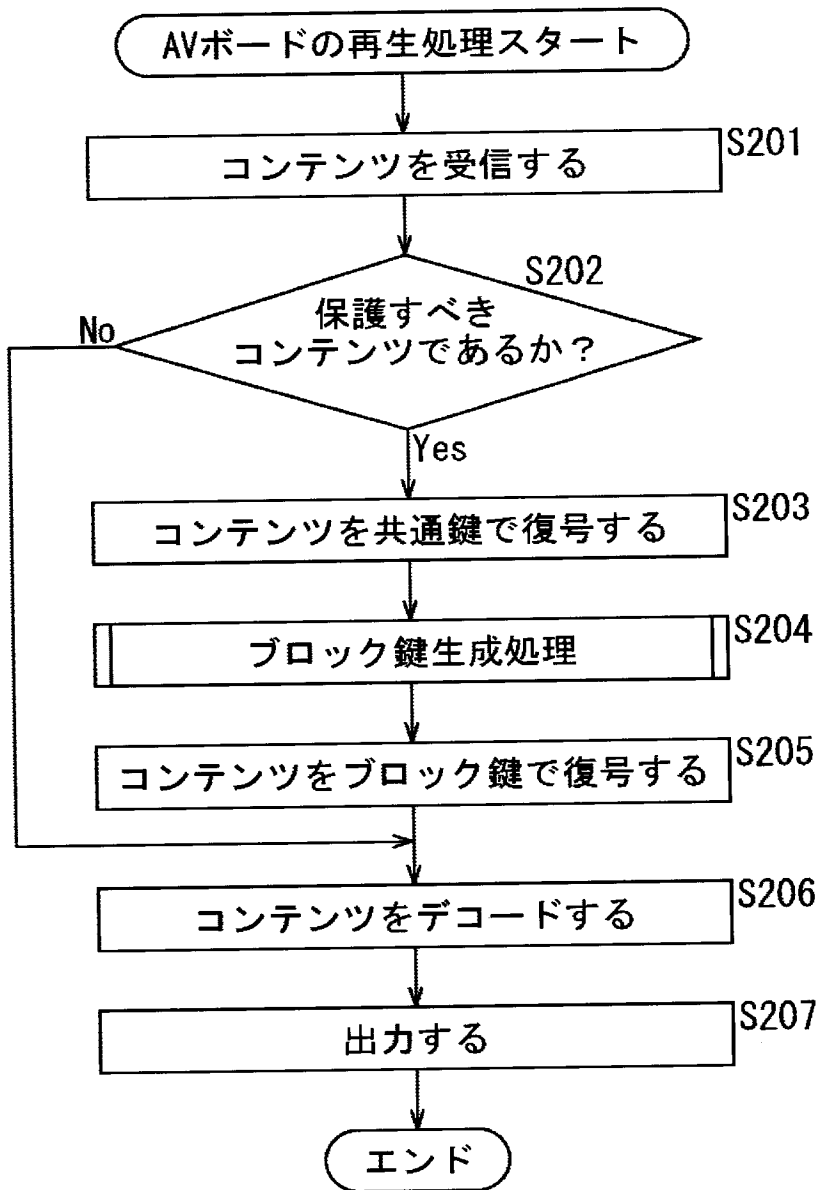
【図18】
図18



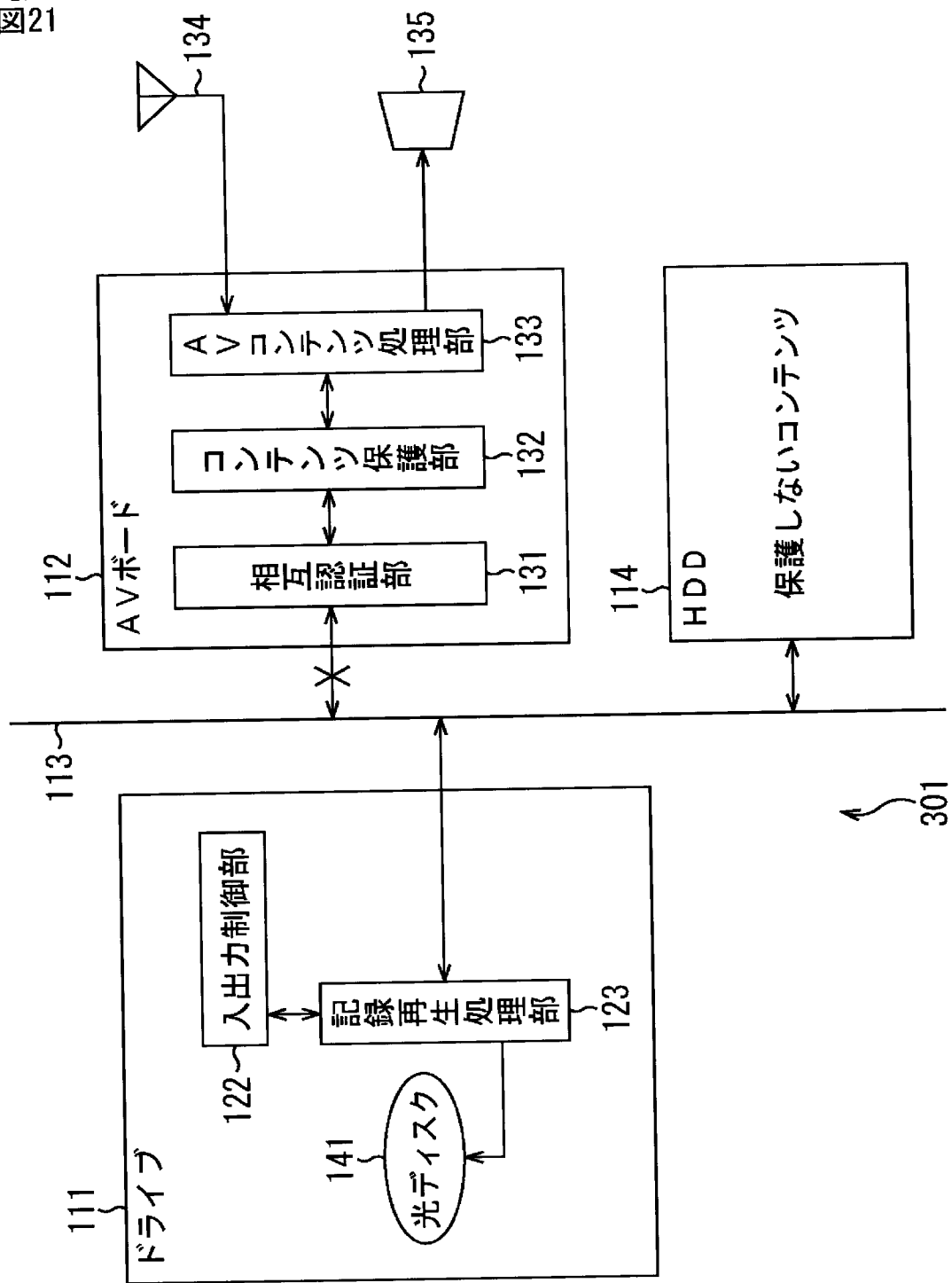
【図19】
図19



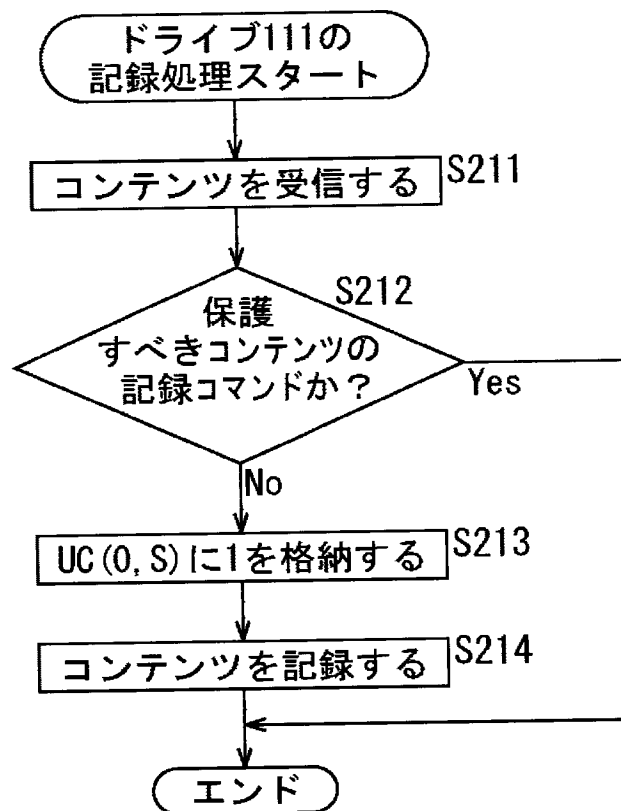
【図20】
図20



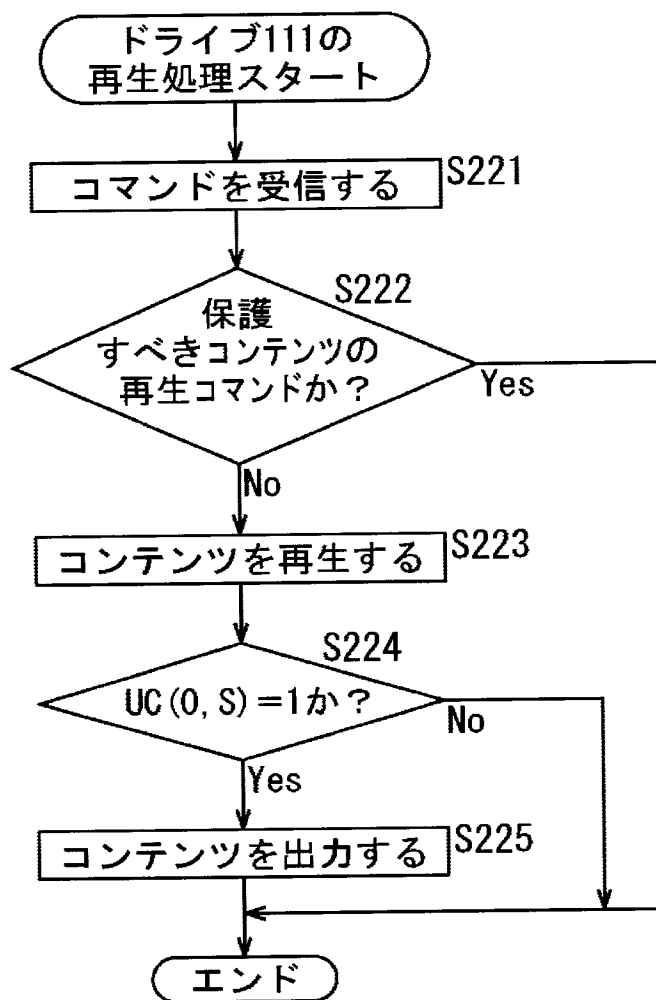
【図 2 1】
図21



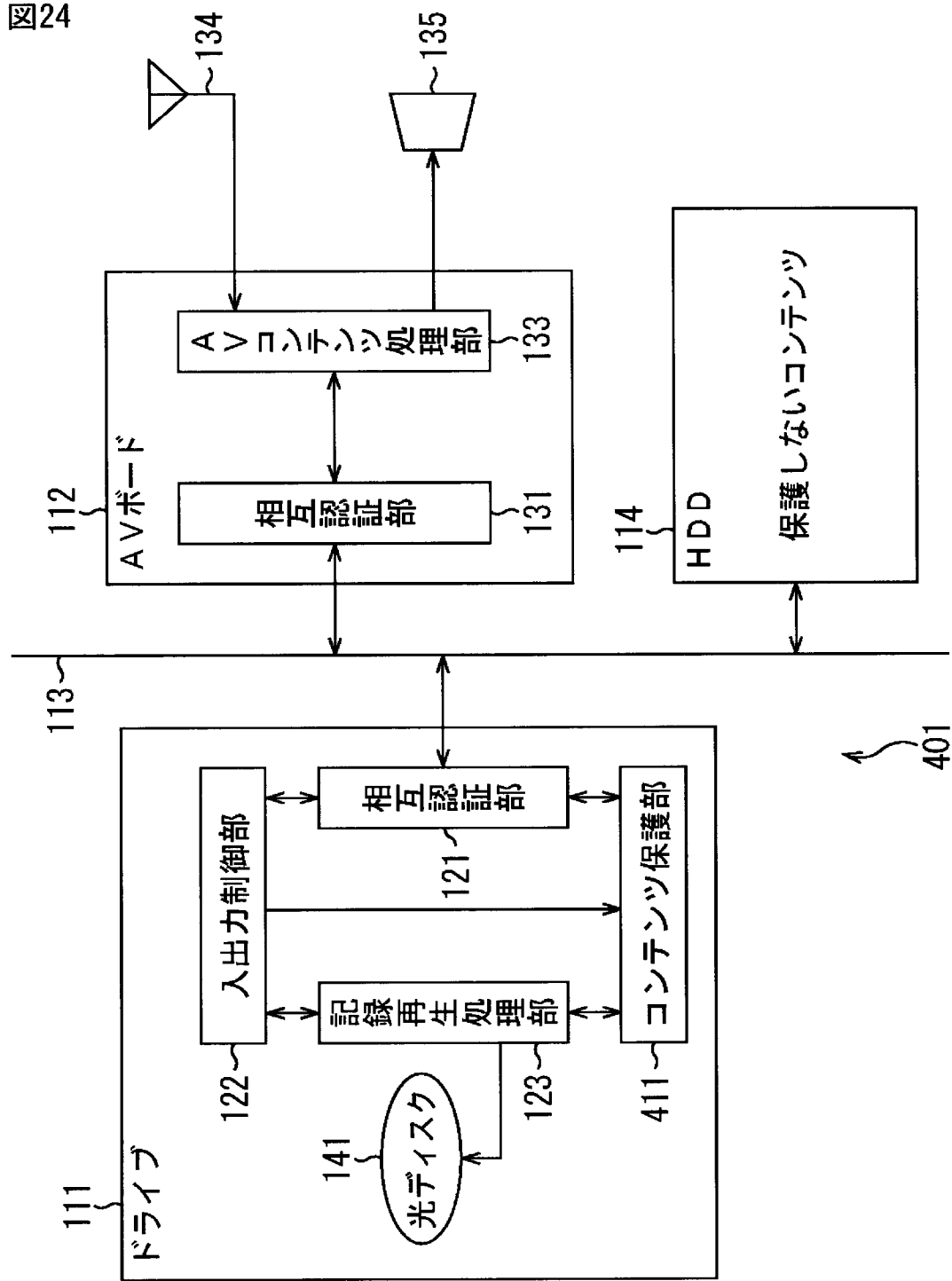
【図22】
図22



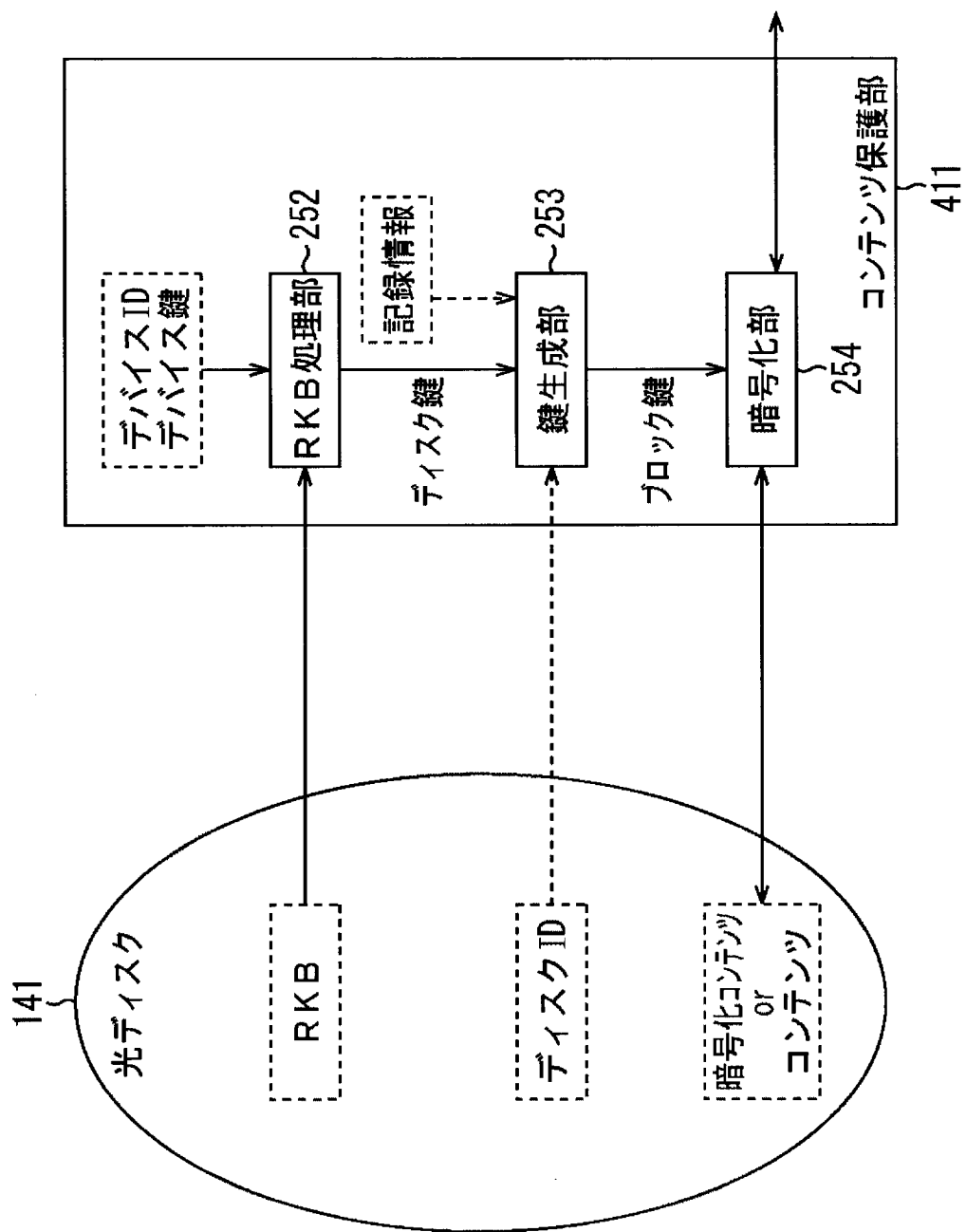
【図23】
図23



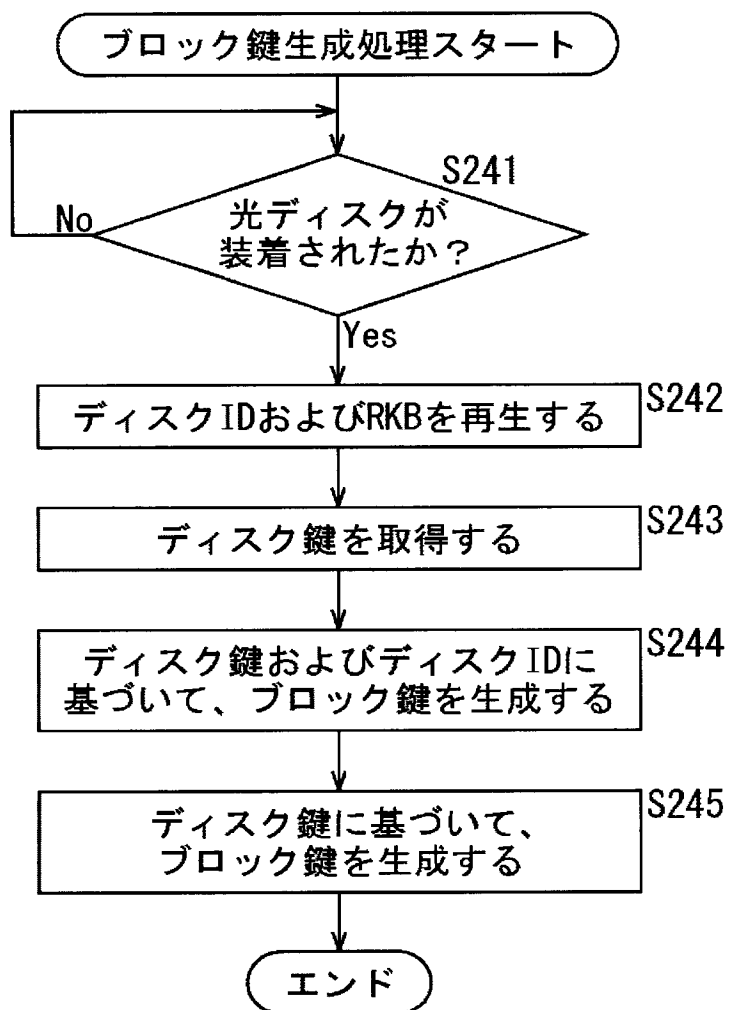
【図24】
図24



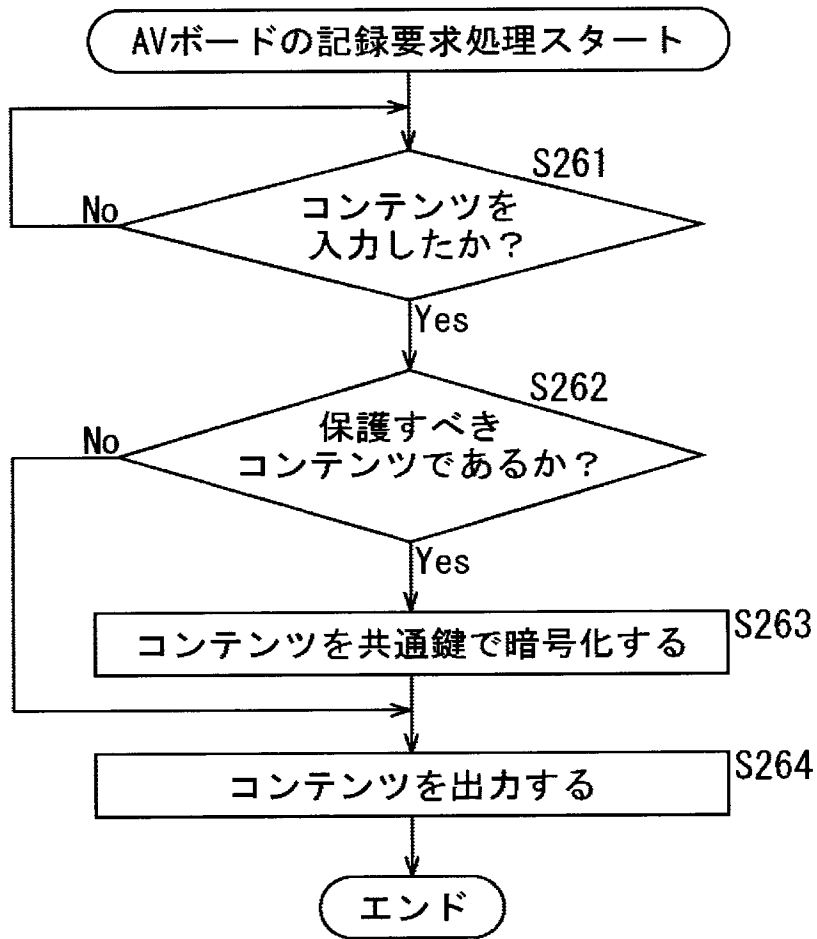
【図25】
図25



【図26】
図26

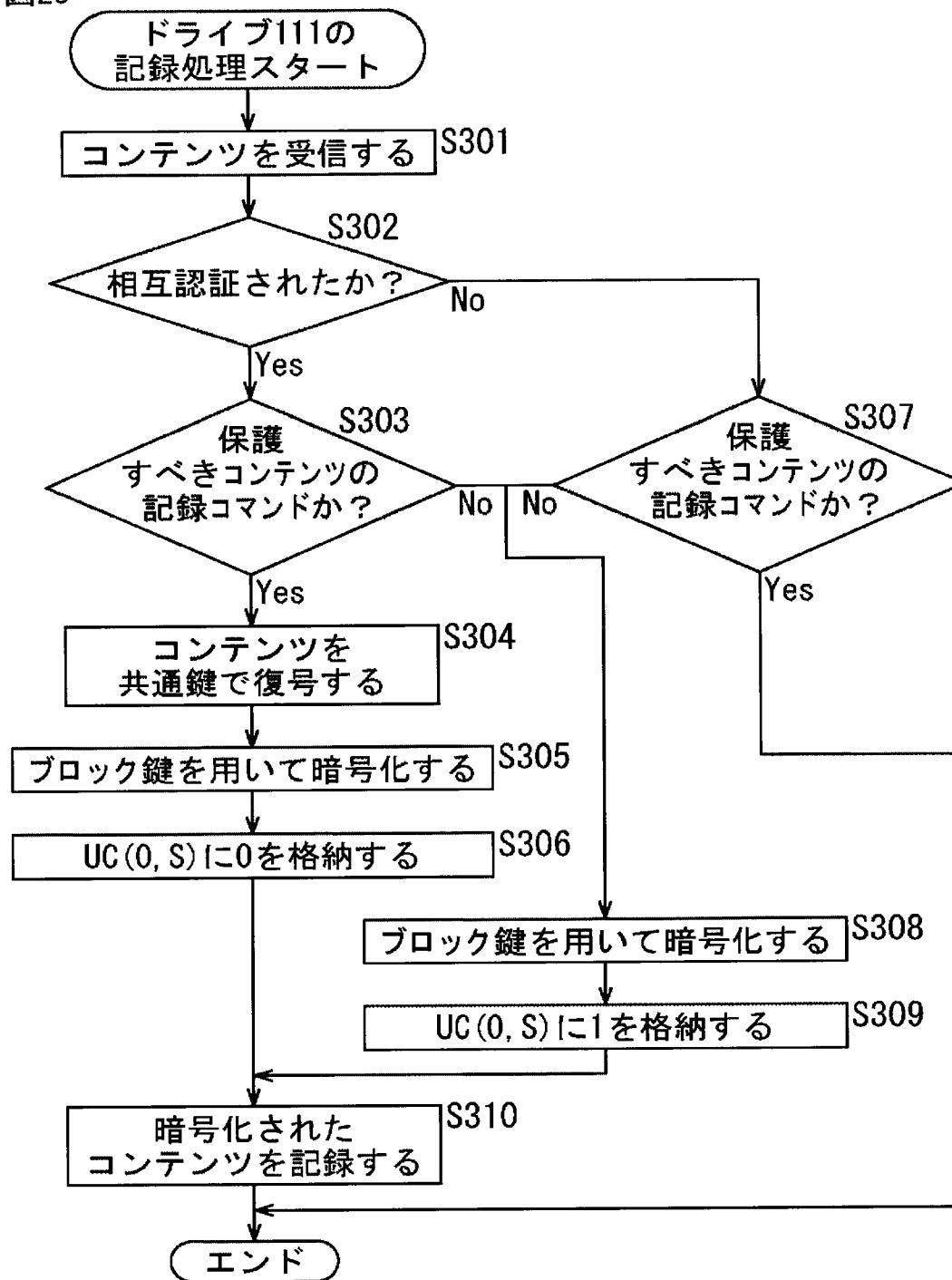


【図 27】
図27



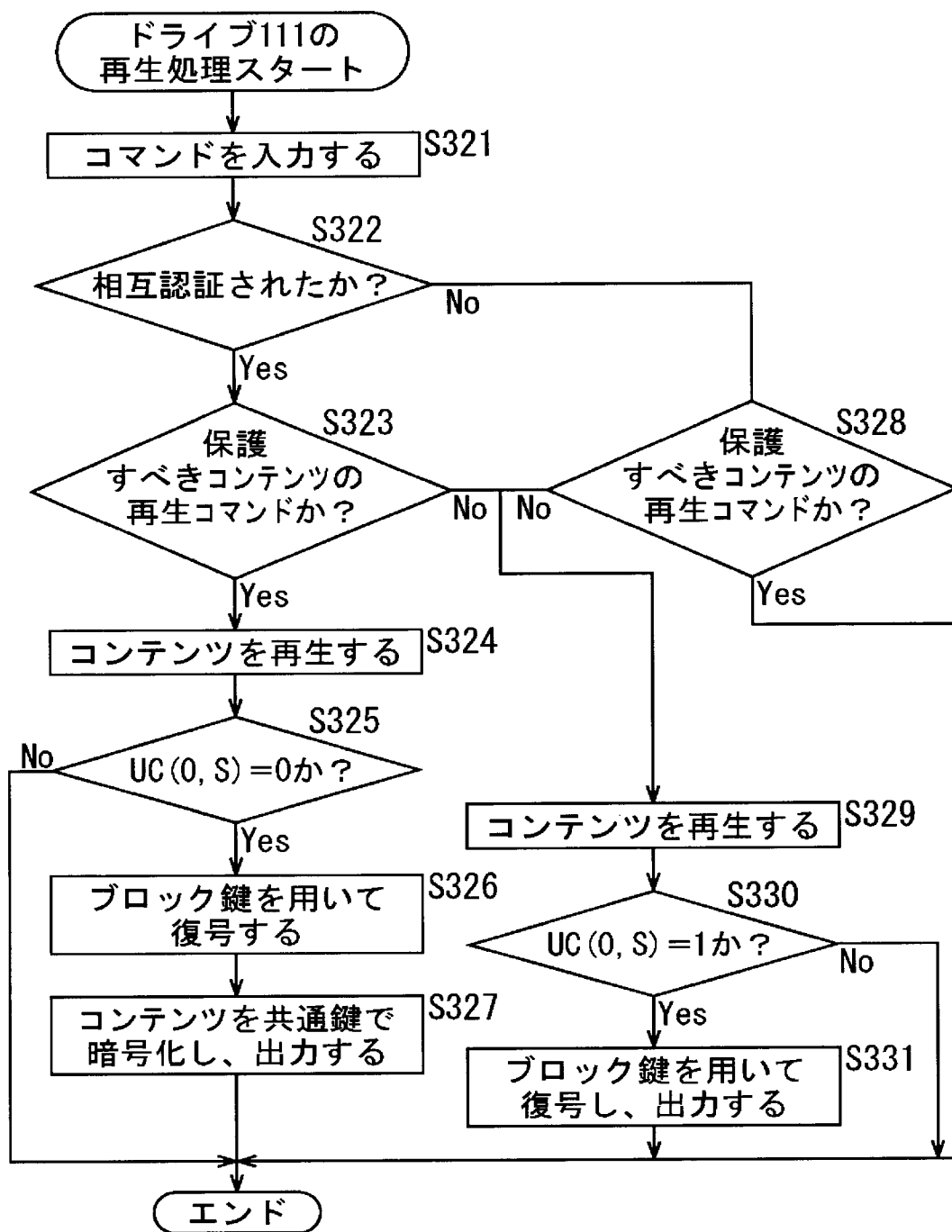
【図28】

図28

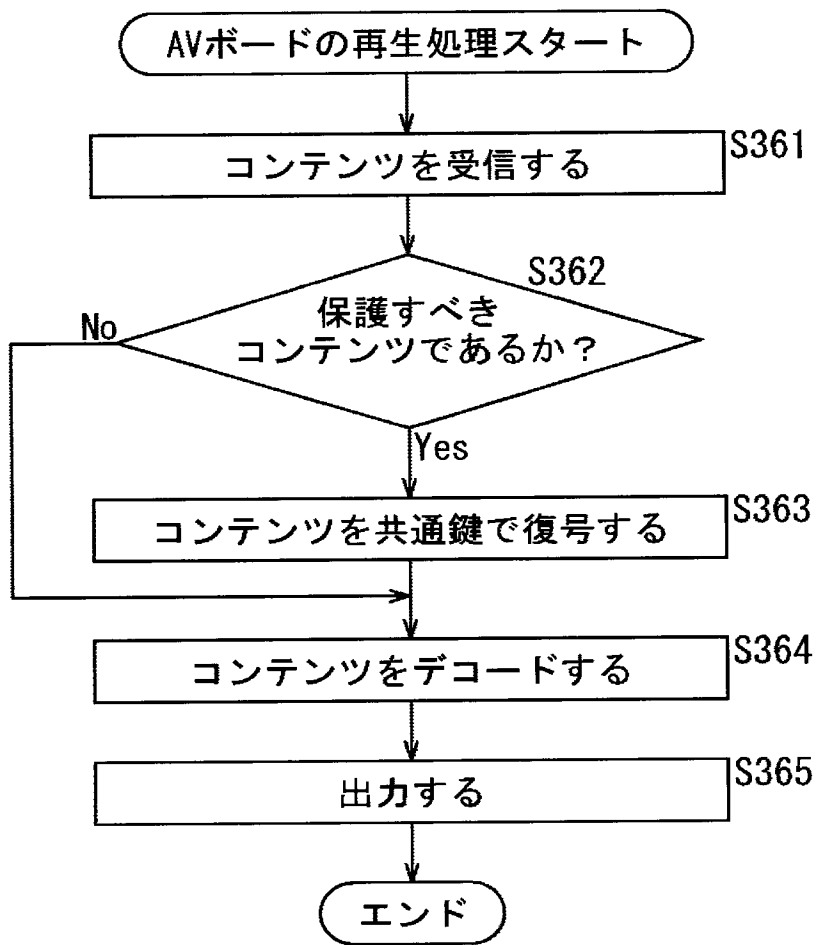


【図29】

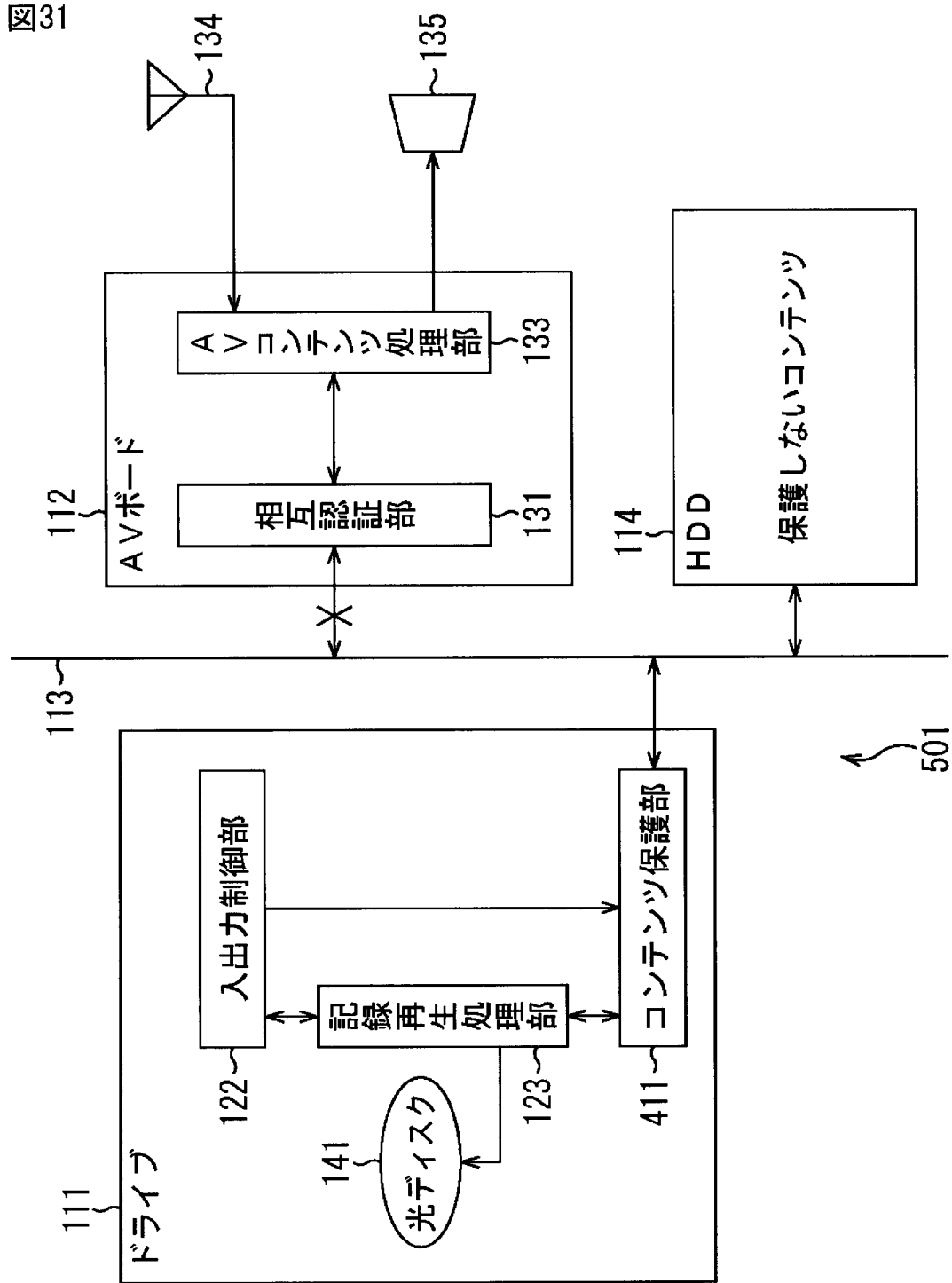
図29



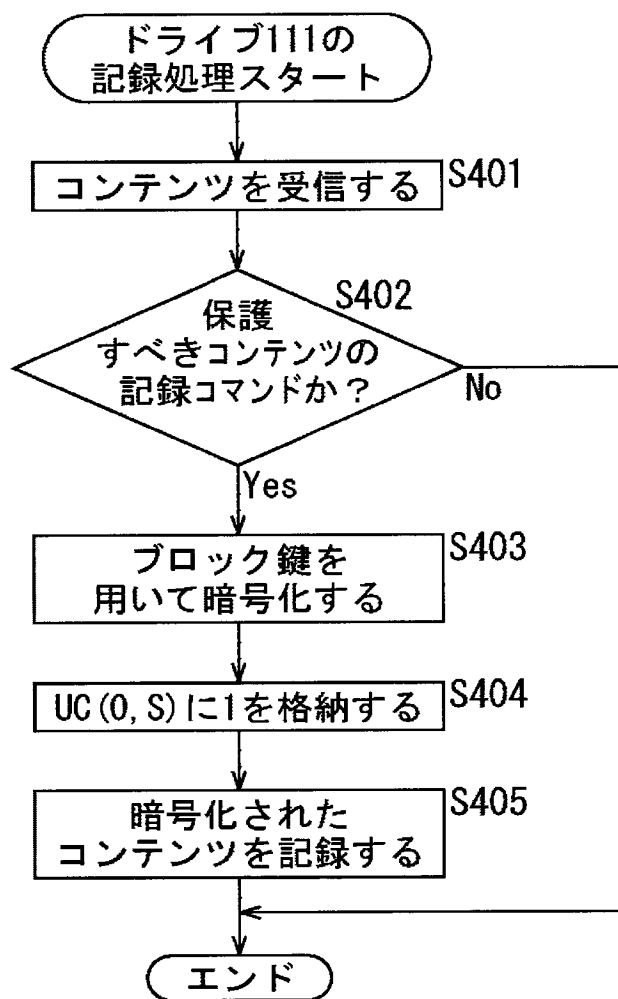
【図30】
図30



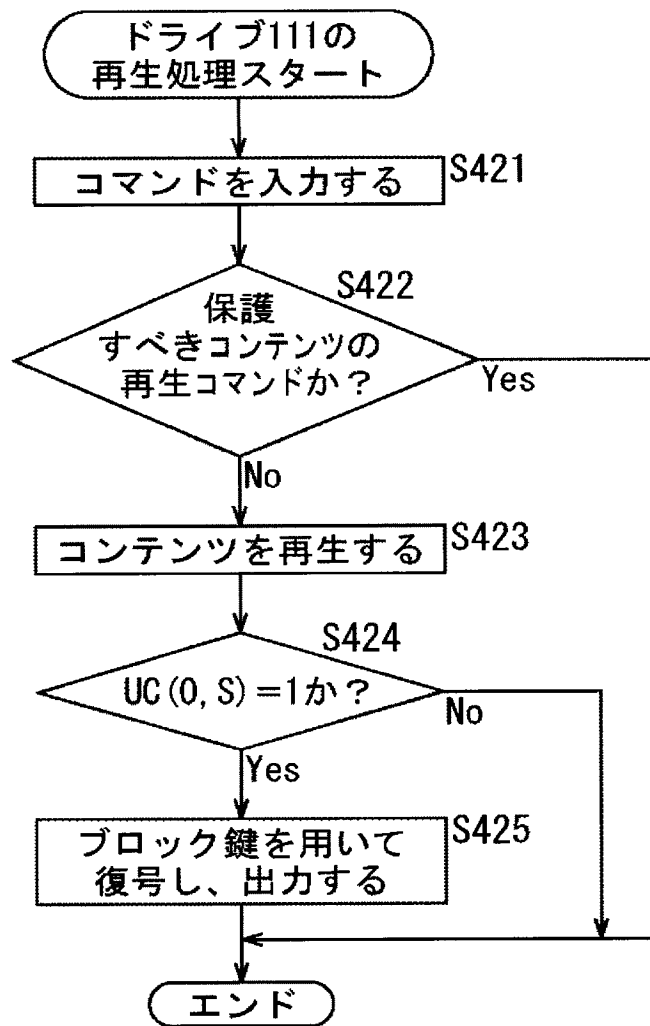
【图 3 1】
图 31



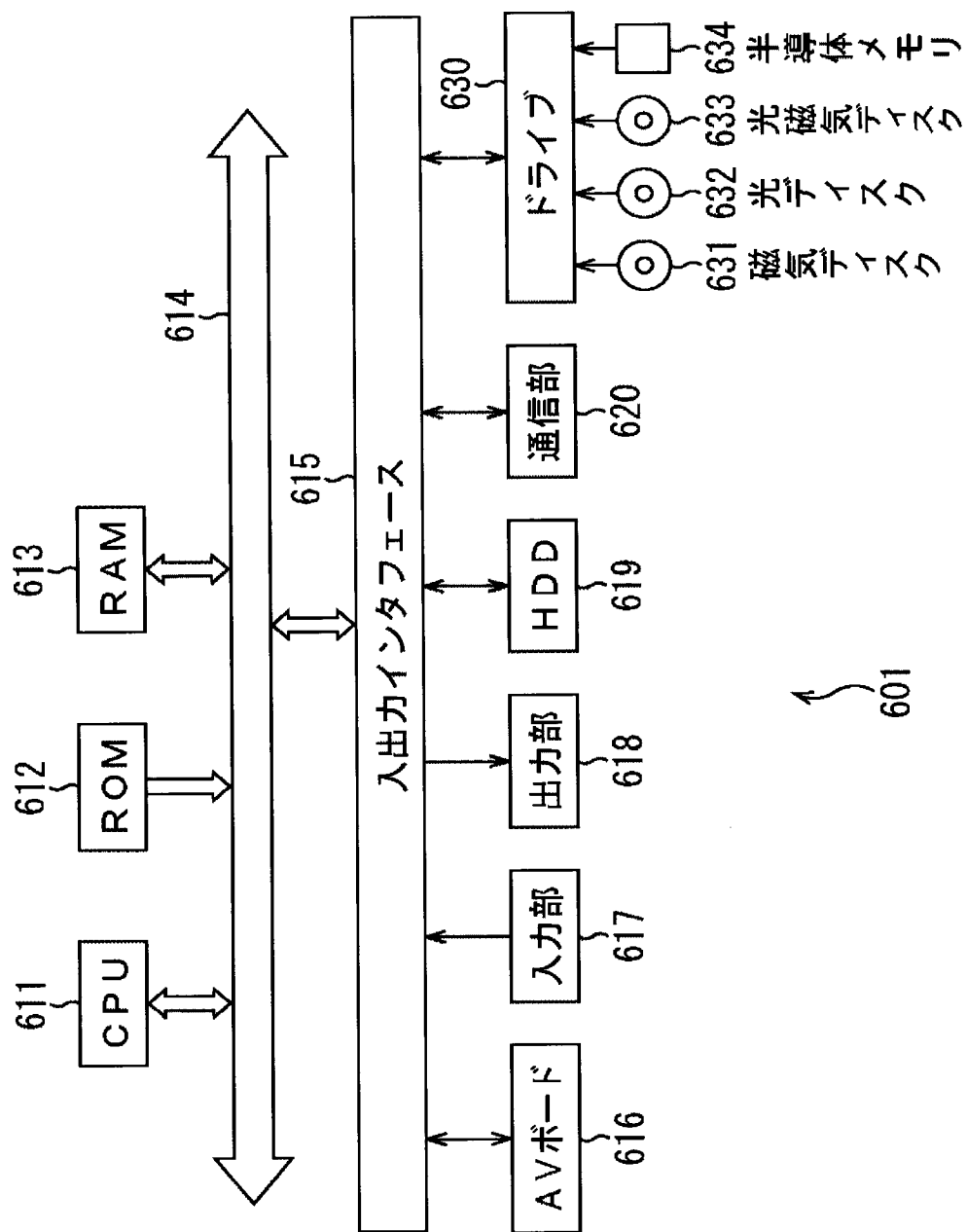
【図 3 2】
図32



【図 3 3】
図33



【図 3 4】
図 34



[Fig. 1] 11: DRIVE, 21: RECORDING/PLAYBACK PROCESSOR, 41: OPTICAL DISC, 12: AV BOARD, 31: AV CONTENT PROCESSOR, 32: CONTENT PROTECTOR

[Fig. 2] 11: DRIVE, 21: RECORDING/PLAYBACK PROCESSOR, 41: OPTICAL DISC, 12: AV BOARD, 31: AV CONTENT PROCESSOR, 32: CONTENT PROTECTOR, 71: HDD, DISC ID 16B, (RKB) SEVERAL MB, ENCRYPTED CONTENT 20GB, PROGRAM, SEVERAL KB,

[Fig. 3] 11: DRIVE, 21: RECORDING/PLAYBACK PROCESSOR, 41: OPTICAL DISC, 91: MUTUAL AUTHENTICATION UNIT, 12: AV BOARD, 31: AV CONTENT PROCESSOR, 32: CONTENT PROTECTOR, 92: MUTUAL AUTHENTICATION UNIT, 71: HDD, CONTENT THAT DOES NOT HAVE TO BE PROTECTED

[Fig. 4] 111: DRIVE, 123: RECORDING/PLAYBACK PROCESSOR, 141: OPTICAL DISC, 121: MUTUAL AUTHENTICATION UNIT, 122: INPUT/OUTPUT CONTROLLER, 112: AV BOARD, 133: AV CONTENT PROCESSOR, 132: CONTENT PROTECTOR, 131: MUTUAL AUTHENTICATION UNIT, 114: HDD, CONTENT THAT DOES NOT HAVE TO BE PROTECTED

[Fig. 5] 201: USER DATA, 32 FRAMES \times 2048 BYTES, 32 SECTORS, 202: USER CONTROL DATA, 32 \times 18 BYTES, 203: DATA FRAME, 32 FRAMES \times 2048 BYTES, + 4-BYTE EDC, 204: PHYSICAL ADDRESS, 16 \times 9 BYTES, 205: SCRAMBLE DATA FRAME, 32 FRAMES \times 2052 BYTES, 206: DATA BLOCK, 304 COLUMNS \times 216 ROWS, 207: LDC BLOCK, 304-COLUMN \times 216-ROW DATA, 32-ROW PARITY, 208: LDC CLUSTER, 152 COLUMNS \times 496 ROWS, 210: ACCESS BLOCK, 24 COLUMNS \times 30

ROWS, 211: BIS BLOCK, 24-COLUMN × 30-ROW DATA, 32-ROW PARITY,
212: BIS CLUSTER, 3 COLUMNS × 496 ROWS, 209-1, 209-2, 209-3,
209-4: LDC 38 COLUMNS, 213-1, 213-2, 213-3: BIS 1 LINES, 496
ROWS, ECC CLUSTER (155 COLUMNS), 496 RECORDING FRAMES,
PHYSICAL CLUSTER (1932 CHANNEL BITS = 1288 DATA BITS)

[Fig. 6] 2048 USER DATA, 2052 BYTES

[Fig. 7] 2052 BYTES, 32 FRAMES

[Fig. 8] 18 BYTES

[Fig. 9] 141: OPTICAL DISC, DISC ID, ENCRYPTED CONTENT OR
CONTENT, 132: CONTENT PROTECTOR, DEVICE ID, DEVICE KEY, 252:
RKB PROCESSOR, DISC KEY, RECORDING INFORMATION, 253: KEY
GENERATOR, BLOCK KEY, 254: ENCRYPTION UNIT, CONTENT

[Fig. 10] DEVICE

[Fig. 11] VERSION (Version), INDEX, ENCRYPTED KEY,
VERSION (Version), INDEX, ENCRYPTED KEY,

[Fig. 12] GENERATION (Generation), INDEX, ENCRYPTED KEY,
RECORDING MEDIUM, DECRYPT, DEVICE 0

[Fig. 13] START MUTUAL AUTHENTICATION BY AV BOARD, S11:
GENERATE COMMON KEY, S12: ENCRYPT COMMON KEY, S13: GENERATE
SIGNATURE TO COMMON KEY, S14: READ AV-BOARD DIGITAL
CERTIFICATE, S15: SEND COMMON KEY, SIGNATURE TO COMMON KEY
AND AV-BOARD DIGITAL CERTIFICATE TO DRIVE, END

[Fig. 14] START MUTUAL AUTHENTICATION BY DRIVE, S31: DECRYPT
RECEIVED AV-BOARD DIGITAL CERTIFICATE, S32: IS AV BOARD
AUTHORIZED ?, S33: DECRYPT COMMON KEY WITH PRIVATE KEY OF

DRIVE, S34: DECRYPT SIGNATURE TO COMMON KEY WITH AV-BOARD
PUBLIC KEY, S35: DOES COMMON KEY MATCH COMMON KEY PROVIDED
WITH SIGNATURE ?, S36: STORE COMMON KEY, END

[Fig. 15] START RECORDING REQUEST PROCESSING BY AV BOARD,
S101: HAS CONTENT BEEN INPUT ?, S102: IS CONTENT TO BE
PROTECTED ?, S103: BLOCK-KEY GENERATION PROCESSING, S104:
ENCRYPT CONTENT WITH BLOCK KEY, S105: ENCRYPT CONTENT WITH
COMMON KEY, S106: OUTPUT CONTENT, END

[Fig. 16] START BLOCK-KEY GENERATION PROCESSING, S121:
REQUEST DISC ID AND RKB, S122: DECRYPT DISC ID AND RKB WITH
COMMON KEY, S123: OBTAIN DISC KEY, S124: GENERATE BLOCK KEY,
RETURN

[Fig. 17] START DISC-INFORMATION PLAYBACK PROCESSING, S141:
RECEIVE REQUEST, S142: MUTUALLY AUTHORIZED ?, S143: PLAYBACK
DISC ID AND RKB, S144: ENCRYPT DISC ID AND RKB WITH COMMON
KEY AND OUTPUT THEM, END

[Fig. 18] START RECORDING PROCESSING BY DRIVE 111, S161:
RECEIVE CONTENT, S162: MUTUALLY AUTHORIZED ?, S163: IS
RECORDING COMMAND FOR CONTENT TO BE PROTECTED ?, S164:
DECRYPT CONTENT WITH COMMON KEY, S165: STORE 0 IN UC(0,S),
S166: IS RECORDING COMMAND FOR CONTENT TO BE PROTECTED ?,
S167: STORE 1 IN UC(0,S), S168: STORE CONTENT, END

[Fig. 19] START PLAYBACK PROCESSING BY DRIVE 111, S191:
INPUT COMMAND, S192: MUTUALLY AUTHORIZED ?, S193: IS
PLAYBACK COMMAND FOR CONTENT TO BE PROTECTED ?, S194:

PLAYBACK CONTENT, S195: UC(0,S)=0 ?, S196: ENCRYPT CONTENT
WITH COMMON KEY AND OUTPUT CONTENT, S197: IS PLAYBACK
COMMAND FOR CONTENT TO BE PROTECTED ?, 198: PLAYBACK CONTENT,
S199: UC(0,S)=1 ?, S200: OUTPUT CONTENT, END

[Fig. 20] START PLAYBACK PROCESSING BY AV BOARD, S201:
RECEIVE CONTENT, S202: IS CONTENT TO BE PROTECTED ?, S203:
DECRYPT CONTENT WITH COMMON KEY, S204: BLOCK-KEY GENERATION
PROCESSING, S205: DECRYPT CONTENT WITH BLOCK KEY, S206:
DECODE CONTENT, S207: OUTPUT, END

[Fig. 21] 111: DRIVE, 123: RECORDING/PLAYBACK PROCESSOR,
141: OPTICAL DISC, 122: INPUT/OUTPUT CONTROLLER, 112: AV
BOARD, 133: AV CONTENT PROCESSOR, 132: CONTENT PROTECTOR,
131: MUTUAL AUTHENTICATION UNIT, 114: HDD, CONTENT THAT DOES
NOT HAVE TO BE PROTECTED

[Fig. 22] START RECORDING PROCESSING BY DRIVE 111, S211:
RECEIVE CONTENT, S212: IS RECORDING COMMAND FOR CONTENT TO
BE PROTECTED ?, S213: STORE 1 IN UC(0,S), S214: STORE
CONTENT, END

[Fig. 23] START PLAYBACK PROCESSING BY DRIVE 111, S221:
RECEIVE COMMAND, S222: IS PLAYBACK COMMAND FOR CONTENT TO BE
PROTECTED ?, S223: PLAYBACK CONTENT, S224: UC(0,S)=1 ?,
S225: OUTPUT CONTENT, END

[Fig. 24] 111: DRIVE, 121: MUTUAL AUTHENTICATION UNIT, 123:
RECORDING/PLAYBACK PROCESSOR, 141: OPTICAL DISC, 122:
INPUT/OUTPUT CONTROLLER, 411: CONTENT PROTECTOR, 112: AV

BOARD, 133: AV CONTENT PROCESSOR, 131: MUTUAL AUTHENTICATION
UNIT, 114: HDD, CONTENT THAT DOES NOT HAVE TO BE PROTECTED
[Fig. 25] 141: OPTICAL DISC, DISC ID, ENCRYPTED CONTENT OR
CONTENT, 411: CONTENT PROTECTOR, DEVICE ID, DEVICE KEY, 252:
RKB PROCESSOR, DISC KEY, RECORDING INFORMATION, 253: KEY
GENERATOR, BLOCK KEY, 254: ENCRYPTION UNIT

[Fig. 26] START BLOCK-KEY GENERATION PROCESSING, S241: IS
OPTICAL DISC LOADED ?, S242: PLAYBACK DISC ID AND RKB, S243:
OBTAIN DISC KEY, S244: GENERATE BLOCK KEY BASED ON DISC KEY
AND DISK ID, S245: GENERATE BLOCK KEY BASED ON DISC KEY, END

[Fig. 27] START RECORDING REQUEST PROCESSING BY AV BOARD,
S261: HAS CONTENT BEEN INPUT ?, S262: IS CONTENT TO BE
PROTECTED ?, S263: ENCRYPT CONTENT WITH COMMON KEY, S264:
OUTPUT CONTENT, END

[Fig. 28] START RECORDING PROCESSING BY DRIVE 111, S301:
RECEIVE CONTENT, S302: MUTUALLY AUTHORIZED ?, S303: IS
RECORDING COMMAND FOR CONTENT TO BE PROTECTED ?, S304:
DECRYPT CONTENT WITH COMMON KEY, S305: ENCRYPT CONTENT WITH
BLOCK KEY, S306: STORE 0 IN UC(0,S), S307: IS RECORDING
COMMAND FOR CONTENT TO BE PROTECTED ?, S308: ENCRYPT CONTENT
WITH BLOCK KEY, S309: STORE 1 IN UC(0,S), S310: STORE
ENCRYPTED CONTENT, END

[Fig. 29] START PLAYBACK PROCESSING BY DRIVE 111, S321:
INPUT COMMAND, S322: MUTUALLY AUTHORIZED ?, S323: IS
PLAYBACK COMMAND FOR CONTENT TO BE PROTECTED ?, S324:

PLAYBACK CONTENT, S325: UC(0,S)=0 ?, S326: DECRYPT CONTENT WITH BLOCK KEY, S327: ENCRYPT CONTENT WITH COMMON KEY AND OUTPUT CONTENT, S328: IS PLAYBACK COMMAND FOR CONTENT TO BE PROTECTED ?, S329: PLAYBACK CONTENT, S330: UC(0,S)=1 ?, S331: DECRYPT CONTENT WITH BLOCK KEY AND OUTPUT CONTENT, END
[Fig. 30] START PLAYBACK PROCESSING BY AV BOARD, S361: RECEIVE CONTENT, S362: IS CONTENT TO BE PROTECTED ?, S363: DECRYPT CONTENT WITH COMMON KEY, S364: DECODE CONTENT, S365: OUTPUT, END

[Fig. 31] 111: DRIVE, 123: RECORDING/PLAYBACK PROCESSOR, 141: OPTICAL DISC, 122: INPUT/OUTPUT CONTROLLER, 411: CONTENT PROTECTOR, 112: AV BOARD, 133: AV CONTENT PROCESSOR, 131: MUTUAL AUTHENTICATION UNIT, 114: HDD, CONTENT THAT DOES NOT HAVE TO BE PROTECTED

[Fig. 32] START RECORDING PROCESSING BY DRIVE 111, S401: RECEIVE CONTENT, S402: IS RECORDING COMMAND FOR CONTENT TO BE PROTECTED ?, S403: ENCRYPT CONTENT WITH BLOCK KEY, S404: STORE 1 IN UC(0,S), S405: STORE ENCRYPTED CONTENT, END

[Fig. 33] START PLAYBACK PROCESSING BY DRIVE 111, S421: INPUT COMMAND, S422: IS PLAYBACK COMMAND FOR CONTENT TO BE PROTECTED ?, 423: PLAYBACK CONTENT, S424: UC(0,S)=1 ?, S425: DECRYPT CONTENT WITH BLOCK KEY AND OUTPUT CONTENT, END

[Fig. 34] 615: INPUT/OUTPUT INTERFACE, 616: AV BOARD, 617: INPUT UNIT, 618: OUTPUT UNIT, 620: COMMUNICATION UNIT, 630: DRIVE, 631: MAGNETIC DISC, 632: OPTICAL DISC, 633: MAGNETO-

OPTICAL DISK, 634: SEMICONDUCTOR MEMORY

[Name of Document] ABSTRACT

[Abstract]

[Object] Content can be flexibly protected according to whether or not the content should be protected.

[Solving Means] When mutual authentication is conducted with an AV board 112 by a mutual authentication unit 121 and when the content input into the mutual authentication unit 121 is encrypted with a common key, an input/output controller 122 determines that the content to be input via a bus 113 is to be protected on the bus 113. The input/output controller 122 then controls a recording/playback processor 123 to generate protection information "0" in user control data US(0,S) corresponding to the content, indicating that the content is to be protected on the bus 113, and records the generated protection information on an optical disc 141 together with the content. The present invention can be applied to an optical-disc recording/playback apparatus.

[Selected Figure] Fig. 4